Kaspersky Anti-Virus 2012

Manuel de l'utilisateur

VERSION DE L'APPLICATION : 12.0

Chers utilisateurs,

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

Ce document peut être modifié sans un avertissement préalable. La version la plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse http://www.kaspersky.com/fr/docs.

Date d'édition : 19/04/11

http://www.kaspersky.com/fr
http://support.kaspersky.com/fr

CONTENU

PRESENTATION DU GUIDE

Les experts de Kaspersky Lab vous souhaitent la bienvenue.

Ce guide contient les informations sur l'installation, sur la configuration et sur l'utilisation de l'application Kaspersky Anti-Virus. Nous espérons que les informations présentées dans ce guide vous aideront à travailler avec l'application.

Ce guide est conçu pour les buts suivants :

- Aider à installer Kaspersky Anti-Virus, activer et utiliser l'application ;
- Offrir un accès rapide aux informations pour répondre aux questions liées à l'application ;
- Présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir une assistance technique.

Pour une utilisation réussie de l'application, la possession des connaissances de base sur l'utilisation de l'ordinateur est requise : connaissance de l'interface du système d'exploitation utilisé, maîtrise des principales tâches, maîtrise du courrier électronique et d'Internet.

DANS CETTE SECTION

CONTENU DU GUIDE

Ce guide contient les sections suivantes.

Sources d'informations sur l'application

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Web que vous pouvez consulter pour discuter du fonctionnement de l'application.

Kaspersky Anti-Virus

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des composants. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés. La section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

Installation et suppression de l'application

Cette section fournit des informations sur l'installation et la suppression de l'application.

Licence de l'application

Cette section présente les principaux concepts liés à l'activation de l'application. Cette section explique le rôle du contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la durée de validité de la licence.

Interface de l'application

Cette section contient des informations sur les principaux éléments de l'interface utilisateur graphique : icône de l'application et menu contextuel, fenêtre principale, fenêtre de configuration et fenêtres de notification.

Lancement et arrêt de l'application

Cette section explique comment lancer et comment arrêter l'application.

Administration de la protection de l'ordinateur

Cette section explique comment déterminer la présence de menaces contre la sécurité de l'ordinateur et comment configurer le niveau de protection. Vous apprendrez comment activer ou désactiver la protection et comment la suspendre temporairement pendant l'utilisation de l'application.

Résolution des problèmes types

Cette section contient des informations sur l'exécution des principales tâches liées à la protection de l'ordinateur à l'aide de l'application.

Configuration étendue de l'application

Cette section contient les informations complémentaires sur la configuration des paramètres de chaque composant de l'application.

Vérification du fonctionnement de l'application

Cette section explique comment vérifier le fonctionnement de l'application : confirmer la détection des virus et de leurs modifications ainsi que l'exécution de l'action requise sur ces derniers.

Contacter le Support technique

Cette section contient des informations sur les méthodes de contact du service d'assistance technique de Kaspersky Lab.

Annexes

Cette section contient des renseignements qui viennent compléter le contenu principal du document.

Glossaire

Cette section contient une liste des termes qui apparaissent dans ce document et leur définition.

Kaspersky Lab

Cette section contient des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers

Cette section contient des informations sur le code tiers utilisé dans l'application.

Index

Cette section permet de trouver rapidement les informations souhaitées dans le document.

CONVENTIONS

Le texte du document est suivi des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions indésirables potentielles qui peuvent amener à la perte des informations ou à la perturbation du fonctionnement de l'ordinateur.
Il est conseillé d'utiliser ...	Les remarques sont encadrées. Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes ou des cas particuliers importants dans le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT+F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
Pour planifier une tâche, procédez comme suit :	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : `Indiquez la date au format JJ:MM:AA.`	Les types suivants du texte apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
`<adresse IP de votre ordinateur>`	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Web que vous pouvez consulter pour discuter du fonctionnement de l'application.

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- page du site de Kaspersky Lab ;
- page sur le site du support technique (base de connaissances) ;
- aide électronique ;
- documentation.

Si vous ne trouvez pas la réponse à votre question, vous pouvez contacter le service d'assistance technique de Kaspersky Lab" (cf. section "Assistance technique par téléphone" à la page 137).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Web de Kaspersky Lab.

Page du site de Kaspersky Lab

Le site Web de Kaspersky Lab contient une page particulière pour chaque application.

La page (http://www.kaspersky.com/fr/kaspersky_anti-virus) fournit des informations générales sur l'application, ces possibilités et ses particularités.

La page http://www.kaspersky.com/fr/ contient le lien sur la boutique en ligne. Le lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

Page sur le site du support technique (banque de solutions)

La Base de connaissances est une section du site Internet du Support Technique contenant les recommandations pour travailler avec les applications de Kaspersky Lab. La Base de connaissance est composée des articles d'aide regroupés selon les thèmes.

La page de l'application dans la Base de connaissances (http://support.kaspersky.com/fr/) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Anti-Virus, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support technique en général.

Aide électronique

L'aide électronique de l'application est composée de fichiers d'aide.

L'aide contextuelle contient les informations sur chaque fenêtre de l'application : la liste et la description des paramètres et la liste des tâches à effectuer.

La version complète de l'aide contient les informations détaillées sur l'administration de la protection de l'ordinateur à l'aide de l'application.

Documentation

Le guide de l'utilisateur contient les informations sur l'installation, sur l'activation, sur la configuration des paramètres, ainsi que les informations pour travailler avec l'application. Le document décrit l'interface graphique et décrit l'exécution des tâches les plus fréquentes dans l'utilisation de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications dans notre forum (http://forum.kaspersky.com/).

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection, sur l'achat ou sur la prolongation de la durée d'utilisation de l'application, vous pouvez contacter nos experts du service commercial à l'aide d'un des moyens suivants :

- En appelant notre service clientèle Français (détails sur http://www.kaspersky.com/fr/contacts).
- En envoyant un message avec votre question par courrier électronique http://www.kaspersky.com/fr/contacts.

La réponse sera formalisée en Français ou en anglais suivant votre demande.

CONTACTER LE GROUPE DE REDACTION DE LA DOCUMENTATION PAR COURRIER ELECTRONIQUE

Pour contacter le Groupe de rédaction de la documentation, vous pouvez envoyer un message par courrier électronique docfeedback@kaspersky.com. En tant que sujet du message, il faut indiquer "Kaspersky Help Feedback: Kaspersky Anti-Virus".

KASPERSKY ANTI-VIRUS

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des composants. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés. La section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

DANS CETTE SECTION

NOUVEAUTES

Les nouveautés suivantes sont présentes dans Kaspersky Anti-Virus :

- L'interface améliorée de la fenêtre principale de Kaspersky Anti-Virus assure un accès rapide aux fonctions de l'application.
- L'amélioration de la logique du fonctionnement de la quarantaine et de la sauvegarde (cf. page 114) : elles sont maintenant représentées sur deux onglets et exécutent différentes actions.
- L'ajout d'un Gestionnaire de tâches pour l'administration simplifiée des tâches de Kaspersky Anti-Virus (cf. section "Administration des tâches d'analyse. Gestionnaire de tâches" à la page 73).
- La participation à Kaspersky Security Network (cf. page 129) permet de définir la réputation des applications et des sites Web sur la base des données obtenues auprès d'utilisateurs issus du monde entier.
- Lorsque l'Antivirus Internet fonctionne, il est possible d'activer séparément l'analyse heuristique pour contrôler les pages Web sur la présence d'hameçonnage (phishing) (cf. section "Utilisation de l'analyse heuristique lors du fonctionnement de l'Antivirus Internet" à la page 95). Avec cela, lors du contrôle de la présence d'hameçonnage (phishing), l'analyse heuristique sera utilisée quel que soit état de l'analyse heuristique (activé ou désactivé) de l'Antivirus Internet.
- La modification de l'apparence de Kaspersky Gadget (cf. page 36).

DISTRIBUTION

Vous pouvez acheter l'application sous une des formes suivantes :

- **Dans une boîte**. Le produit est distribué via notre réseau de partenaires.
- **Via la boutique en ligne**. L'application peut être achetée via la boutique en ligne de Kaspersky Lab (http://www.kaspersky.com/fr, section **Boutique en ligne**) ou via le site d'un partenaire.

Si vous achetez le produit en boîte, vous recevez les éléments suivants :

- pochette cachetée contenant le cédérom d'installation où sont enregistrés les fichiers de l'application et la documentation de l'application ;

- bref guide de l'utilisateur contenant le code d'activation de l'application ;
- contrat de licence reprenant les conditions d'utilisation de l'application.

Ces éléments peuvent varier en fonction du pays où l'application est diffusée.

Si vous achetez Kaspersky Anti-Virus via la boutique en ligne, vous devrez télécharger l'application depuis le site Internet. Les informations indispensables à l'activation de l'application vous seront envoyées par courrier électronique après le paiement.

Pour en savoir plus sur les modes d'achat et de distribution, contactez notre Service Ventes.

SERVICE POUR LES UTILISATEURS ENREGISTRES

L'achat d'une licence vous donne le statut d'utilisateur enregistré tout au long de la durée de sa validité, ce qui vous permet de bénéficier des services suivants :

- Mise à jour des bases et nouvelles versions de l'application ;
- Support par téléphone et par courrier électronique sur toutes les questions en rapport avec l'installation, la configuration et l'utilisation de l'application ;
- Notification sur les nouvelles applications de Kaspersky Lab et les nouveaux virus référencés. Afin bénéficier de ce service, vous devrez vous abonner à la liste de diffusion des informations de Kaspersky Lab ZAO présente sur le site Internet du service d'assistance technique.

Aucun support ne sera apporté sur l'utilisation du système d'exploitation ou des logiciels tiers.

CONFIGURATIONS LOGICIELLES ET MATERIELLES

Afin de garantir un fonctionnement optimal de Kaspersky Anti-Virus, votre ordinateur doit répondre au minimum à la configuration suivante :

Configuration générale :

- 480 Mo d'espace disponible sur le disque dur (dont 380 Mo pour le disque système).
- CD-/DVD-ROM (pour l'installation de Kaspersky Anti-Virus depuis un cédérom).
- Connexion à Internet (pour l'activation de l'application et la mise à jour des bases ou modules de l'application).
- Microsoft Internet Explorer 6.0 ou suivant.
- Microsoft Windows Installer 2.0.

Exigences pour les systèmes d'exploitation Microsoft Windows XP Home Edition (Service Pack 2 ou suivant), Microsoft Windows XP Professional (Service Pack 2 ou suivant), Microsoft Windows XP Professional x64 Edition (Service Pack 2 ou suivant) :

- Processeur Intel Pentium 800 MHz 32 bits (x86)/ 64 bits (x64) ou supérieur (ou analogue compatible) ;
- 512 Mo de mémoire vive disponible.

Exigences pour les systèmes d'exploitation Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate,

Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate :

- Processeur Intel Pentium 1 GHz 32 bits (x86)/ 64 bits (x64) ou supérieur (ou analogue compatible).
- 1 Go de mémoire vive disponible (pour les systèmes d'exploitation de 32 bits) ; 2 Go de mémoire vive disponible (pour les systèmes d'exploitation de 64 bits).

Exigences pour les netbooks :

- Processeur Intel Atom 1.6 GHz ou analogue compatible.
- Carte vidéo Intel GMA950 avec une mémoire d'au moins 64 Mo (ou analogue compatible).
- Ecran de 10.1 pouces minimum.

INSTALLATION ET SUPPRESSION DE L'APPLICATION

Cette section fournit des informations sur l'installation et la suppression de l'application.

DANS CETTE SECTION

PROCEDURE D'INSTALLATION STANDARD

L'installation de Kaspersky Anti-Virus s'opère en mode interactif à l'aide d'un Assistant d'installation.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Si l'application doit protéger plus d'un ordinateur (le nombre maximum d'ordinateurs protégés dépend de votre licence), elle sera alors installée de la même manière sur tous les ordinateurs. Notez que dans ce cas, la durée de validité de la licence commence à partir de la première activation de l'application, conformément aux termes du contrat de licence. Lors de l'activation de l'application sur le deuxième ordinateur et les suivants, la durée de validité de la licence est réduite de la durée écoulée depuis la première activation. Ainsi, la licence arrivera à échéance en même temps pour toutes les copies installées.

- *Pour installer Kaspersky Anti-Virus sur votre ordinateur,*

  exécutez le fichier d'installation (fichier avec extension exe) présent sur le CD-ROM de l'application.

La procédure d'installation de Kaspersky Anti-Virus depuis une version téléchargée via Internet est en tout point identique au processus d'installation depuis le CD-ROM.

DANS CETTE SECTION

ETAPE 1. RECHERCHER D'UNE VERSION PLUS RECENTE DE L'APPLICATION

Avant l'installation, Kaspersky Anti-Virus vérifie la présence d'une version de l'application plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si les serveurs de Kaspersky Lab n'hébergent pas de version plus récente, l'Assistant d'installation de la version actuelle est lancé.

Si les serveurs de mises à jour hébergent une version plus récente, vous serez invité à la télécharger et à l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application, afin de bénéficier des nouvelles améliorations. Ces améliorations permettent de protéger votre ordinateur d'une manière plus efficace. Si vous refusez d'installer la version plus récente, l'Assistant d'installation de la version actuelle sera lancé. Si vous décidez d'installer la nouvelle version, les fichiers de la distribution seront copiés sur votre ordinateur et l'Assistant d'installation de la nouvelle version sera lancé automatiquement. Pour connaître les avantages de la version plus récente, lisez la documentation correspondant à l'application.

ETAPE 2. VERIFICATION DE LA CONFIGURATION DU SYSTEME PAR RAPPORT A LA CONFIGURATION REQUISE

Avant d'installer Kaspersky Anti-Virus, le programme vérifie si le système d'exploitation et les paquets de mises à jour (Service Pack) installés correspondent à la configuration requise pour l'installation (cf. section "Configurations logicielle et matérielle" à la page 15). De plus, l'application vérifie les privilèges (droits) pour l'installation du logiciel. Si une des conditions énumérées n'est pas remplie, un message apparaîtra.

Si l'ordinateur correspond aux pré-requis, l'Assistant exécute la recherche des applications de Kaspersky Lab dont l'utilisation commune avec Kaspersky Anti-Virus peut amener à l'apparition de conflits. Si de telles applications sont découvertes, vous devrez les supprimer manuellement.

Si la liste des applications contient une version antérieure de Kaspersky Anti-Virus ou de Kaspersky Internet Security, toutes les données qui peuvent être utilisées par Kaspersky Anti-Virus 2012 (par exemple, informations sur l'activation ou paramètres de l'application) seront enregistrées et utilisées pendant l'installation, et l'application installée antérieurement sera automatiquement supprimée.

ETAPE 3. SELECTION DU TYPE D'INSTALLATION

Cette étape de l'installation permet de choisir le type d'installation de Kaspersky Anti-Virus qui vous convient le mieux :

- *Installation standard*. Si vous sélectionnez cette option (la case **Modifier les paramètres d'installation** n'est pas cochée), l'application sera complètement installée sur l'ordinateur, avec les paramètres recommandés par les experts de Kaspersky Lab.

- *Installation avec possibilité de modification des paramètres*. Dans ce cas (la case **Modifier les paramètres d'installation est installée**), vous pourrez indiquer le dossier dans lequel l'application doit être installée (cf. section "Etape 7. Sélection du dossier d'installation" cf. page 19), et si nécessaire, activer la protection du processus d'installation (cf. section "Etape 8. Préparation de l'installation" à la page 20).

Afin de poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 4. LECTURE DU CONTRAT DE LICENCE

Au cours de cette étape, vous devez prendre connaissance du contrat de licence conclu entre vous et Kaspersky Lab.

Lisez attentivement le contrat et si vous en acceptez toutes les dispositions, cliquez sur **J'accepte**. L'installation de l'application se poursuivra.

Si vous n'êtes pas d'accord avec le contrat de licence, alors annulez l'installation de l'application en cliquant sur le bouton **Annuler**.

ETAPE 5. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Cette étape est une invitation à participer au programme Kaspersky Security Network. La participation au programme implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces découvertes sur l'ordinateur, sur les applications exécutées, sur les applications signées et les informations relatives au système. Aucune donnée personnelle n'est transmise.

Lisez les dispositions relatives à l'utilisation de Kaspersky Security Network. Pour lire le texte complet du contrat, cliquez sur le bouton **Accord KSN complet**. Si vous êtes d'accord avec tous les points, cochez la case dans la fenêtre de l'Assistant **J'accepte les conditions de participation à Kaspersky Security Network**.

Cliquez sur le bouton **Suivant**, si vous exécutez l'installation avec possibilité de modification des paramètres (cf. la section Etape 3. Sélection du type d'installation" à la page 18). Pour l'installation standard, cliquez sur le bouton **Installer**. L'installation continuera.

ETAPE 6. RECHERCHE D'APPLICATIONS INCOMPATIBLES

Au cours de cette étape, le programme d'installation recherche des applications incompatibles avec Kaspersky Anti-Virus.

Si ces applications n'existent pas, l'Assistant passe automatiquement à l'étape suivante.

Si des applications incompatibles sont détectées, une liste sera affichée sur l'écran et vous aurez la possibilité de les supprimer. Les applications que Kaspersky Anti-Virus ne peut supprimer automatiquement doivent être supprimées manuellement. Au cours de la suppression des applications incompatibles, le redémarrage du système sera requis. Ensuite, l'installation de Kaspersky Anti-Virus se poursuivra automatiquement.

Afin de poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 7. SELECTION DU DOSSIER D'INSTALLATION

Cette étape de l'Assistant d'installation est proposée uniquement en cas d'installation avec possibilité de modification des paramètres (cf. section Etape 3. Sélection du type d'installation" à la page 18). Cette étape est sautée pendant l'installation standard et l'application est installée dans le dossier par défaut.

Cette étape correspond à la sélection du dossier dans lequel Kaspersky Anti-Virus sera installé. Le chemin d'accès suivant est proposé par défaut :

- **<disque>\Program Files\ Kaspersky Lab\Kaspersky Anti-Virus 2012** pour les systèmes 32 bits ;
- **<disque>\Program Files (x86)\ Kaspersky Lab\Kaspersky Anti-Virus 2012** pour les systèmes 64 bits.

Pour installer Kaspersky Anti-Virus dans un autre dossier, saisissez le nouveau chemin d'accès dans le champ ou cliquez sur le bouton **Parcourir** et choisissez le dossier dans la fenêtre qui s'ouvre.

Prêtez attention aux restrictions suivantes :

- Il est interdit d'installer l'application sur des disques de réseau ou des disques amovibles ou sur des disques virtuels (créés à l'aide de l'instruction `SUBST`).
- Il est déconseillé d'installer l'application dans un dossier contenant des fichiers et d'autres dossiers car l'accès à ceux-ci pourrait être bloqué après l'installation pour la modification.
- Le chemin d'accès au dossier d'installation doit compter moins de 160 caractères et ne peut pas contenir les caractères suivants **/**, **?**, **:**, *****, **"**, **>**, **<** et **|.**

Si vous souhaitez savoir si vous disposez d'assez de place sur le disque pour installer l'application, cliquez sur **Disque**. La fenêtre qui s'ouvre fournit les informations relatives à l'espace disque. Cliquez sur **OK** pour fermer la fenêtre.

Pour poursuivre l'installation, cliquez sur le bouton **Suivant** dans la fenêtre de l'Assistant.

ETAPE 8. PREPARATION DE L'INSTALLATION

Cette étape de l'Assistant d'installation est proposée uniquement en cas d'installation avec possibilité de modification des paramètres (cf. section Etape 3. Sélection du type d'installation" à la page 18). Lors de l'installation standard, cette étape est ignorée.

Dans la mesure où des applications malveillantes capables de gêner l'installation de Kaspersky Anti-Virus pourraient être présentes sur l'ordinateur, le processus d'installation doit être protégé.

Par défaut, la protection du processus d'installation est activée : la case **Protéger l'installation de l'application** est cochée dans la fenêtre de l'Assistant.

Il est conseillé de décocher cette case s'il est impossible d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop). La protection activée peut en être la cause.

Dans ce cas, interrompez l'installation et relancez l'installation de l'application dès le début, cochez la case **Modifier les paramètres d'installation** à l'étape Choix du type d'installation (cf. section "Etape 3. Sélection du type d'installation" à la page 18) et, à l'étape Préparation de l'installation, décochez la case **Protéger l'installation de l'application**.

Afin de poursuivre l'installation, cliquez sur **Installer**.

Lors de l'installation de l'application sur un ordinateur fonctionnant sous le système d'exploitation Microsoft Windows XP, les connexions de réseau en cours seront interrompues. La majorité des connexions interrompues seront rétablies automatiquement après quelques secondes.

ETAPE 9. INSTALLATION

L'installation de l'application peut durer un certain temps. Attendez jusqu'à la fin avant de passer à l'étape suivante.

Une fois l'installation terminée, l'Assistant passe automatiquement à l'étape suivante.

En cas d'erreurs d'installation qui pourraient être provoquées par la présence sur l'ordinateur de programmes malveillants empêchant l'installation de logiciels antivirus, l'Assistant d'installation proposera de télécharger un outil spécial pour éliminer l'infection : *l'utilitaire Kaspersky Virus Removal Tool*.

Si vous êtes d'accord avec l'installation de l'utilitaire, l'Assistant le téléchargera depuis les serveurs de Kaspersky Lab. Ensuite, l'installation de l'utilitaire sera lancée automatiquement. Si l'Assistant ne parvient pas à télécharger l'utilitaire, vous aurez la possibilité de le télécharger vous-même en cliquant sur le lien proposé.

Une fois que l'utilitaire aura terminé son travail, il faut le supprimer et relancer l'installation de Kaspersky Anti-Virus depuis le début.

ETAPE 10. FIN DE L'INSTALLATION

Cette fenêtre de l'Assistant vous signale la fin de l'installation de l'application. Pour commencer à utiliser Kaspersky Anti-Virus, assurez-vous que la case **Lancer Kaspersky Anti-Virus 2012** est cochée, puis cliquez sur le bouton Terminer.

Dans certains cas, le redémarrage du système d'exploitation peut être requis. Si la case **Lancer Kaspersky Anti-Virus 2012** est cochée, l'application sera lancée automatiquement après le redémarrage.

Si, avant la fin de l'Assistant, vous avez décoché la case, l'application doit être lancée manuellement (cf. section "Lancement et arrêt manuel du fonctionnement de l'application" à la page 38).

ETAPE 11. ACTIVATION DE L'APPLICATION

L'*activation* est une procédure qui correspond à insérer un code dans le logiciel Kaspersky Lab afin d'en activer sa licence. Cette licence donne le droit d'utiliser la version commerciale de l'application pendant la durée de validité de la licence.

Une connexion à Internet est indispensable pour activer l'application.

Vous pouvez choisir parmi les options suivantes pour activer Kaspersky Anti-Virus:

- **Activer la version commerciale**. Sélectionnez cette option et saisissez le code d'activation si vous avez acheté la version commerciale de l'application.

  Si vous saisissez le code d'activation de Kaspersky Internet Security, la procédure de permutation sur Kaspersky Internet Security sera lancée à la fin de l'activation.

- **Activer la version d'évaluation**. Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter la version commerciale. Vous pouvez utiliser toutes les fonctionnalités de l'application pendant la période définie par la licence de la version d'évaluation. Après la date d'expiration de la licence, vous ne pourrez plus activer la version d'évaluation.

ETAPE 12. ENREGISTREMENT DE L'UTILISATEUR

Cette étape est accessible uniquement lors de l'activation de la version commerciale de l'application. Lors de l'activation de la version d'évaluation, cette étape est passée.

Si vous souhaitez pouvoir bénéficier de l'aide du Support technique de Kaspersky Lab, il faudra vous enregistrer.

Si vous acceptez de vous enregistrer, saisissez les données requises dans les champs correspondants, puis cliquez sur le bouton **Suivant**.

ETAPE 13. FIN DE L'ACTIVATION

L'Assistant vous signale la réussite de l'activation de Kaspersky Anti-Virus. Il propose également des informations sur la licence : type (commerciale, évaluation, etc.), fin de validité de la licence et nombre d'ordinateurs couverts par cette licence.

En cas d'activation par l'abonnement, les informations relatives à la durée de validité de la licence sont fournies en plus des informations sur l'état de l'abonnement.

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

MISE A JOUR DE LA VERSION PRECEDENTE DE KASPERSKY ANTI-VIRUS

Si votre ordinateur est déjà équipé de Kaspersky Anti-Virus 2010 ou 2011, vous devez réaliser une mise à niveau vers Kaspersky Anti-Virus 2012. Si vous possédez une licence valide de Kaspersky Anti-Virus 2010 ou 2011, il n'est pas nécessaire d'activer l'application : l'Assistant d'installation reçoit automatiquement les informations sur la licence de Kaspersky Anti-Virus 2010 ou 2011 et les utilise dans le cadre de l'installation.

L'installation de Kaspersky Anti-Virus s'opère en mode interactif à l'aide d'un Assistant d'installation.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Si l'application doit protéger plus d'un ordinateur (le nombre maximum d'ordinateurs protégés dépend de votre licence), elle sera alors installée de la même manière sur tous les ordinateurs. Notez que dans ce cas, la durée de validité de la licence commence à partir de la première activation de l'application, conformément aux termes du contrat de licence. Lors de l'activation de l'application sur le deuxième ordinateur et les suivants, la durée de validité de la licence est réduite de la durée écoulée depuis la première activation. Ainsi, la licence arrivera à échéance en même temps pour toutes les copies installées.

- *Pour installer Kaspersky Anti-Virus sur votre ordinateur,*

  exécutez le fichier d'installation (fichier avec extension exe) présent sur le CD-ROM de l'application.

  La procédure d'installation de Kaspersky Anti-Virus depuis une version téléchargée via Internet est en tout point identique au processus d'installation depuis le CD-ROM.

DANS CETTE SECTION

ETAPE 1. RECHERCHER D'UNE VERSION PLUS RECENTE DE L'APPLICATION

Avant l'installation, Kaspersky Anti-Virus vérifie la présence d'une version de l'application plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si les serveurs de Kaspersky Lab n'hébergent pas de version plus récente, l'Assistant d'installation de la version actuelle est lancé.

Si les serveurs de mises à jour hébergent une version plus récente, vous serez invité à la télécharger et à l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application, afin de bénéficier des nouvelles améliorations. Ces améliorations permettent de protéger votre ordinateur d'une manière plus efficace. Si vous refusez d'installer la version plus récente, l'Assistant d'installation de la version actuelle sera lancé. Si vous décidez d'installer la nouvelle version, les fichiers de la distribution seront copiés sur votre ordinateur et l'Assistant d'installation de la nouvelle version sera lancé automatiquement. Pour connaître les avantages de la version plus récente, lisez la documentation correspondant à l'application.

ETAPE 2. VERIFICATION DE LA CONFIGURATION DU SYSTEME PAR RAPPORT A LA CONFIGURATION REQUISE

Avant d'installer Kaspersky Anti-Virus, le programme vérifie si le système d'exploitation et les paquets de mises à jour (Service Pack) installés correspondent à la configuration requise pour l'installation (cf. section "Configurations logicielle et matérielle" à la page 15). De plus, l'application vérifie les privilèges (droits) pour l'installation du logiciel. Si une des conditions énumérées n'est pas remplie, un message apparaîtra.

Si l'ordinateur correspond aux pré-requis, l'Assistant exécute la recherche des applications de Kaspersky Lab dont l'utilisation commune avec Kaspersky Anti-Virus peut amener à l'apparition de conflits. Si de telles applications sont découvertes, vous devrez les supprimer manuellement.

Si la liste des applications contient une version antérieure de Kaspersky Anti-Virus ou de Kaspersky Internet Security, toutes les données qui peuvent être utilisées par Kaspersky Anti-Virus 2012 (par exemple, informations sur l'activation ou paramètres de l'application) seront enregistrées et utilisées pendant l'installation, et l'application installée antérieurement sera automatiquement supprimée.

ETAPE 3. SELECTION DU TYPE D'INSTALLATION

Cette étape de l'installation permet de choisir le type d'installation de Kaspersky Anti-Virus qui vous convient le mieux :

- *Installation standard*. Si vous sélectionnez cette option (la case **Modifier les paramètres d'installation** n'est pas cochée), l'application sera complètement installée sur l'ordinateur, avec les paramètres recommandés par les experts de Kaspersky Lab.

- *Installation avec possibilité de modification des paramètres*. Dans ce cas (la case **Modifier les paramètres d'installation est installée**), vous pourrez indiquer le dossier dans lequel l'application doit être installée (cf. section "Etape 7. Sélection du dossier d'installation" à la page 19), et si nécessaire, activer la protection du processus d'installation (cf. section "Etape 8. Préparation de l'installation" à la page 20).

Afin de poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 4. LECTURE DU CONTRAT DE LICENCE

Au cours de cette étape, vous devez prendre connaissance du contrat de licence conclu entre vous et Kaspersky Lab.

Lisez attentivement le contrat et si vous en acceptez toutes les dispositions, cliquez sur **J'accepte**. L'installation de l'application se poursuivra.

Si vous n'êtes pas d'accord avec le contrat de licence, alors annulez l'installation de l'application en cliquant sur le bouton **Annuler**.

ETAPE 5. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Cette étape est une invitation à participer au programme Kaspersky Security Network. La participation au programme implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces découvertes sur l'ordinateur, sur les applications exécutées, sur les applications signées et les informations relatives au système. Aucune donnée personnelle n'est transmise.

Lisez les dispositions relatives à l'utilisation de Kaspersky Security Network. Pour lire le texte complet du contrat, cliquez sur le bouton **Accord KSN complet**. Si vous êtes d'accord avec tous les points, cochez la case dans la fenêtre de l'Assistant **J'accepte les conditions de participation à Kaspersky Security Network**.

Cliquez sur le bouton **Suivant**, si vous exécutez l'installation avec possibilité de modification des paramètres (cf. la section Etape 3. Sélection du type d'installation" à la page 18). Pour l'installation standard, cliquez sur le bouton **Installer**. L'installation continuera.

ETAPE 6. RECHERCHE D'APPLICATIONS INCOMPATIBLES

Au cours de cette étape, le programme d'installation recherche des applications incompatibles avec Kaspersky Anti-Virus.

Si ces applications n'existent pas, l'Assistant passe automatiquement à l'étape suivante.

Si des applications incompatibles sont détectées, une liste sera affichée sur l'écran et vous aurez la possibilité de les supprimer. Les applications que Kaspersky Anti-Virus ne peut supprimer automatiquement doivent être supprimées manuellement. Au cours de la suppression des applications incompatibles, le redémarrage du système sera requis. Ensuite, l'installation de Kaspersky Anti-Virus se poursuivra automatiquement.

Afin de poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 7. SELECTION DU DOSSIER D'INSTALLATION

Cette étape de l'Assistant d'installation est proposée uniquement en cas d'installation avec possibilité de modification des paramètres (cf. section Etape 3. Sélection du type d'installation" à la page 18). Cette étape est sautée pendant l'installation standard et l'application est installée dans le dossier par défaut.

Cette étape correspond à la sélection du dossier dans lequel Kaspersky Anti-Virus sera installé. Le chemin d'accès suivant est proposé par défaut :

- **<disque>\Program Files\ Kaspersky Lab\Kaspersky Anti-Virus 2012** pour les systèmes 32 bits ;
- **<disque>\Program Files (x86)\ Kaspersky Lab\Kaspersky Anti-Virus 2012** pour les systèmes 64 bits.

Pour installer Kaspersky Anti-Virus dans un autre dossier, saisissez le nouveau chemin d'accès dans le champ ou cliquez sur le bouton **Parcourir** et choisissez le dossier dans la fenêtre qui s'ouvre.

Prêtez attention aux restrictions suivantes :

- Il est interdit d'installer l'application sur des disques de réseau ou des disques amovibles ou sur des disques virtuels (créés à l'aide de l'instruction `SUBST`).
- Il est déconseillé d'installer l'application dans un dossier contenant des fichiers et d'autres dossiers car l'accès à ceux-ci pourrait être bloqué après l'installation pour la modification.
- Le chemin d'accès au dossier d'installation doit compter moins de 160 caractères et ne peut pas contenir les caractères suivants **/**, **?**, **:**, *****, **"**, **>**, **<** et **|.**

Si vous souhaitez savoir si vous disposez d'assez de place sur le disque pour installer l'application, cliquez sur **Disque**. La fenêtre qui s'ouvre fournit les informations relatives à l'espace disque. Cliquez sur **OK** pour fermer la fenêtre.

Pour poursuivre l'installation, cliquez sur le bouton **Suivant** dans la fenêtre de l'Assistant.

ETAPE 8. PREPARATION DE L'INSTALLATION

Cette étape de l'Assistant d'installation est proposée uniquement en cas d'installation avec possibilité de modification des paramètres (cf. section Etape 3. Sélection du type d'installation" à la page 18). Lors de l'installation standard, cette étape est ignorée.

Dans la mesure où des applications malveillantes capables de gêner l'installation de Kaspersky Anti-Virus pourraient être présentes sur l'ordinateur, le processus d'installation doit être protégé.

Par défaut, la protection du processus d'installation est activée : la case **Protéger l'installation de l'application** est cochée dans la fenêtre de l'Assistant.

Il est conseillé de décocher cette case s'il est impossible d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop). La protection activée peut en être la cause.

Dans ce cas, interrompez l'installation et relancez l'installation de l'application dès le début, cochez la case **Modifier les paramètres d'installation** à l'étape Choix du type d'installation (cf. section "Etape 3. Sélection du type d'installation" à la page 18) et, à l'étape Préparation de l'installation, décochez la case **Protéger l'installation de l'application**.

Afin de poursuivre l'installation, cliquez sur **Installer**.

Lors de l'installation de l'application sur un ordinateur fonctionnant sous le système d'exploitation Microsoft Windows XP, les connexions de réseau en cours seront interrompues. La majorité des connexions interrompues seront rétablies automatiquement après quelques secondes.

ETAPE 9. INSTALLATION

L'installation de l'application peut durer un certain temps. Attendez jusqu'à la fin avant de passer à l'étape suivante.

Une fois l'installation terminée, l'Assistant passe automatiquement à l'étape suivante.

En cas d'erreurs d'installation qui pourraient être provoquées par la présence sur l'ordinateur de programmes malveillants empêchant l'installation de logiciels antivirus, l'Assistant d'installation proposera de télécharger un outil spécial pour éliminer l'infection : *l'utilitaire Kaspersky Virus Removal Tool*.

Si vous êtes d'accord avec l'installation de l'utilitaire, l'Assistant le téléchargera depuis les serveurs de Kaspersky Lab. Ensuite, l'installation de l'utilitaire sera lancée automatiquement. Si l'Assistant ne parvient pas à télécharger l'utilitaire, vous aurez la possibilité de le télécharger vous-même en cliquant sur le lien proposé.

Une fois que l'utilitaire aura terminé son travail, il faut le supprimer et relancer l'installation de Kaspersky Anti-Virus depuis le début.

ETAPE 10. FIN DE L'ASSISTANT

Cette fenêtre de l'Assistant vous signale la fin de l'installation de l'application. Pour commencer à utiliser Kaspersky Anti-Virus, assurez-vous que la case **Lancer Kaspersky Anti-Virus 2012** est cochée, puis cliquez sur le bouton Terminer.

Dans certains cas, le redémarrage du système d'exploitation peut être requis. Si la case **Lancer Kaspersky Anti-Virus 2012** est cochée, l'application sera lancée automatiquement après le redémarrage.

Si, avant la fin de l'Assistant, vous avez décoché la case, l'application doit être lancée manuellement (cf. section "Lancement et arrêt manuel du fonctionnement de l'application" à la page 38).

SCENARIOS D'INSTALLATION ATYPIQUES

Cette section décrit des scénarios d'installation de l'application qui se distinguent d'une installation standard ou d'une mise à jour depuis la version précédente.

Installation de Kaspersky Anti-Virus avec activation ultérieure à l'aide du code d'activation de Kaspersky Internet Security

Si pendant l'installation de Kaspersky Anti-Virus à l'étape de l'activation de l'application vous saisissez le code d'activation de Kaspersky Internet Security, la procédure d'extension sera lancée, à l'issue de laquelle Kaspersky Anti-Virus va basculer sur Kaspersky Internet Security.

Si pendant l'installation de Kaspersky Anti-Virus, à l'étape d'activation de l'application, vous avez choisi l'option **Activer plus tard** et puis que vous activez l'application installée avec le code d'activation de Kaspersky Internet Security, la procédure d'extension sera également lancée, à l'issue de laquelle Kaspersky Anti-Virus va basculer sur Kaspersky Internet Security.

Installation de Kaspersky Anti-Virus 2012 sur Kaspersky Internet Security 2010 ou 2011

Si vous lancez l'installation de Kaspersky Anti-Virus 2012 sur un ordinateur déjà équipé de Kaspersky Internet Security 2010 ou 2011 avec une licence valide, l'Assistant d'installation, après avoir récupéré les informations sur la licence, vous proposera de choisir la suite des événements :

- Utiliser la licence valide de Kaspersky Internet Security 2010 ou 2011. Dans ce cas, la procédure d'extension sera lancée à l'issue de laquelle Kaspersky Internet Security 2012 sera installé. Vous pouvez utiliser Kaspersky Internet Security 2012 pendant la durée de validité restante de la licence de Kaspersky Internet Security 2010 ou 2011.

- Poursuivre l'installation de Kaspersky Anti-Virus 2012. Dans ce cas, la procédure d'installation passe à l'étape Activation de l'application selon le scénario standard.

PREMIERE UTILISATION

Après l'installation et l'activation, l'application est prête à l'emploi. Pour garantir un niveau de protection optimal de l'ordinateur, exécutez les opérations suivantes directement après l'installation et l'activation de l'application :

- Mise à jour les bases de l'application (cf. section "Procédure de mise à jour des bases et modules de l'application" à la page 45).

- Rechercher la présence éventuelle de virus (cf. section "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page 48), et de vulnérabilités (cf. section "Procédure de recherche de vulnérabilités sur l'ordinateur" à la page 48) sur l'ordinateur.

- Vérifier l'état de la protection de l'ordinateur et, le cas échéant, éliminer les problèmes de protection.

SUPPRESSION DE L'APPLICATION

Suite à la suppression de Kaspersky Anti-Virus, l'ordinateur et vos données personnelles ne seront plus protégés !

La suppression de Kaspersky Anti-Virus s'effectue à l'aide de l'Assistant d'installation.

Pour lancer l'Assistant,

dans le menu **Démarrer**, sélectionnez l'option **Applications** → **Kaspersky Anti-Virus 2012** →**Supprimer Kaspersky Anti-Virus 2012**.

DANS CETTE SECTION

ETAPE 1. ENREGISTREMENT DE DONNEES POUR UNE REUTILISATION

A cette étape vous pouvez indiquer les données de l'application que vous voulez enregistrer pour l'utilisation suivante lors de la réinstallation de l'application (par exemple, sa version plus récente).

Par défaut, l'application est supprimée entièrement de l'ordinateur.

Pour enregistrer les données en vue de leur réutilisation, procédez comme suit :

1. Sélectionnez l'option **Enregistrer les objets de l'application**.
2. Cochez les cases en regard des données à enregistrer :
   - **Informations sur l'activation** : données permettant de ne pas activer ultérieurement l'application à installer, mais d'utiliser automatiquement la licence actuelle, à condition qu'elle soit toujours valable au moment de l'installation.
   - **Objets de la sauvegarde ou de la quarantaine** : fichiers analysés par l'application et placés dans la sauvegarde ou en quarantaine.
   - **Paramètres** de **fonctionnement de l'application** : valeurs des paramètres de fonctionnement de l'application. Ces paramètres sont définis au cours de la configuration de l'application.
   - **Données iChecker** : fichiers contenant les informations sur les objets déjà soumis à la recherche de virus.

ETAPE 2. CONFIRMATION DE LA SUPPRESSION DU PROGRAMME

Dans la mesure où la suppression de l'application met en danger la protection de l'ordinateur et de vos données personnelles, vous devez confirmer la suppression de l'application. Pour ce faire, cliquez sur le bouton **Supprimer**.

Vous pouvez à tout moment annuler cette action, en cliquant sur le bouton **Annuler**.

ETAPE 3. SUPPRESSION DE L'APPLICATION. FIN DE LA SUPPRESSION

Cette étape de l'Assistant correspond à la suppression de l'application de l'ordinateur. Attendez la fin du processus de suppression.

La suppression peut requérir le redémarrage du système d'exploitation. Si vous décidez de reporter le redémarrage, la fin de la procédure de suppression sera reportée jusqu'au moment où le système d'exploitation sera redémarré ou quand l'ordinateur sera éteint et allumé de nouveau.

LICENCE DE L'APPLICATION

Cette section présente les principaux concepts liés à l'activation de l'application. Cette section explique le rôle du contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la durée de validité de la licence.

DANS CETTE SECTION

PRESENTATION DU CONTRAT DE LICENCE

Le Contrat de licence est un contrat juridique entre vous et Kaspersky Lab ZAO dans lequel les conditions d'utilisation de l'application sont décrites.

Veuillez lire attentivement les conditions du Contrat de licence avant d'utiliser l'application.

Vous pouvez faire connaissance avec les conditions du Contrat de licence lors de l'installation de l'application de Kaspersky Lab.

Il est estimé que vous acceptez les conditions du Contrat de licence dans les situations suivantes :

- En ouvrant la boîte contenant le CD d'installation (uniquement si vous avez acheté l'application en boîte dans les magasins de détail ou dans les magasins de nos partenaires).
- En étant d'accord avec le texte du Contrat de licence lors de l'installation de l'application.

Si vous n'êtes pas d'accord avec les conditions du Contrat de licence, vous devez interrompre l'installation de l'application.

PRESENTATION DES DONNEES

Pour augmenter le niveau de la protection opérationnelle, en acceptant les conditions du contrat de licence, vous acceptez de transmettre automatiquement les informations sur les volumes de contrôle des fichiers traités (MD5), les informations pour définir la réputation de l'URL, ainsi que les données sur la protection contre le courrier indésirable. Les informations obtenues ne contiennent aucunes données personnelles ou autres informations confidentielles. Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi. Pour plus d'informations détaillées, visitez notre site Internet http://support.kaspersky.com/fr/.

PRESENTATION DE LA LICENCE

La *licence* est un droit d'utilisation de l'application octroyé pour une durée définie sur la base du Contrat de licence. La licence contient le code d'activation unique de votre copie de Kaspersky Anti-Virus.

La licence vous donne droit aux types de service suivants :

- Utilisation de l'application sur un ou plusieurs appareils.

  Le nombre d'appareils sur lequel vous pouvez utiliser l'application est défini dans le Contrat de licence.

- Recours au service d'assistance technique de Kaspersky Lab.

- Obtention des services complets proposés par Kaspersky Lab ou par ses partenaires durant la validité de la licence (cf. section "Service pour les utilisateurs enregistrés" à la page 15).

Le volume de services offert et la durée d'utilisation de l'application dépendent du type de licence utilisée pour activer l'application.

Les types de licence suivants existent :

- *Evaluation* : licence gratuite à durée limitée qui permet de prendre connaissance de l'application.

  Si vous copiez l'application depuis le site http://www.kaspersky.com/fr, vous obtenez automatiquement la licence d'évaluation. Une fois que la validité de la licence est écoulée, Kaspersky Anti-Virus arrête de remplir toutes ces fonctions. Pour pouvoir continuer à utiliser l'application, vous devez acheter une licence commerciale.

- *Commerciale :* licence payante à durée déterminée octroyée lors de l'achat de l'application.

  A l'issue de la validité de la licence commerciale, l'application continue à fonctionner, mais avec des fonctionnalités réduites. Vous pouvez toujours soumettre l'ordinateur à une analyse antivirus et utiliser les autres composants de l'application, mais uniquement à l'aide des bases installées avant l'expiration de la licence. Pour pouvoir continuer à utiliser Kaspersky Anti-Virus, il faut renouveler la licence commerciale.

  Il est conseillé de renouveler la durée de validité de la licence avant la date d'expiration de la licence actuelle afin de garantir la protection antivirus maximale de votre ordinateur.

PRESENTATION DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez après avoir acheté une licence commerciale pour Kaspersky Anti-Virus. Ce code est indispensable pour activer l'application.

Le code d'activation est une suite de 20 caractères alphanumériques (alphabet latin) au format XXXXX-XXXXX-XXXXX-XXXXX.

Le mode de livraison du code d'activation dépend de la méthode d'achat de l'application :

- Si vous avez acheté Kaspersky Anti-Virus en magasin, le code d'activation figure dans la documentation présente dans la boîte contenant le cédérom d'installation.

- Si vous avez acheté Kaspersky Anti-Virus en ligne, le code d'activation est envoyé à l'adresse de messagerie que vous avez renseignée lors de la commande.

Le décompte de la durée de validité de la licence débute à partir de l'activation de l'application. Si vous avez acheté une licence prévue pour l'utilisation de Kaspersky Anti-Virus sur plusieurs appareils, le décompte de la durée de validité débute à partir de l'activation sur le premier ordinateur.

Si le code d'activation a été perdu ou supprimé par hasard après l'activation, contactez le Support technique de Kaspersky Lab pour le restaurer. La demande s'effectue depuis Mon Espace Personnel (cf. section "Support technique via Mon Espace Personnel" à la page 137).

Après avoir activé l'application à l'aide du code d'activation, vous recevez un *numéro de client*. Le numéro de client est un numéro d'utilisateur obligatoire pour obtenir le support technique par téléphone ou dans Mon Espace Personnel (cf. section "Support technique via Mon Espace Personnel" à la page 137).

INTERFACE DE L'APPLICATION

Cette section contient des informations sur les principaux éléments de l'interface utilisateur graphique : icône de l'application et menu contextuel, fenêtre principale, fenêtre de configuration et fenêtres de notification.

DANS CETTE SECTION

ICONE DANS LA ZONE DE NOTIFICATION

L'icône de l'application apparaît dans la zone de notification de la barre des tâches de Microsoft Windows directement après son installation.

Dans le système d'exploitation Microsoft Windows 7, l'icône de l'application est dissimulée par défaut. Pour utiliser l'application, vous pouvez l'afficher (cf. la documentation du système d'exploitation).

L'icône remplit les fonctions suivantes :

- Elle indique le fonctionnement de l'application ;
- Elle permet d'accéder au menu contextuel, à la fenêtre principale de l'application et à la fenêtre de consultation des nouvelles.

Indication du fonctionnement de l'application

L'icône indique le fonctionnement de l'application. Elle représente l'état de la protection et montre également plusieurs actions fondamentales exécutées par l'application à l'heure actuelle :

 – analyse d'un message en cours ;

 – analyse du trafic Web en cours ;

 – mise à jour des bases et des modules des applications en cours ;

 – redémarrage de l'ordinateur requis pour appliquer les mises à jour ;

 – échec du fonctionnement d'un composant quelconque de l'application.

L'animation de l'icône est activée par défaut : par exemple, lors de l'analyse du message, l'icône miniature d'un message pulse sur le fond de l'icône de l'application, et lors de la mise à jour des bases de l'application, l'icône du globe tourne. Vous pouvez désactiver l'animation (cf. section "Transparence des fenêtres de notifications" à la page 127).

Si l'animation est désactivée, l'icône peut prendre un des aspects suivants :

(icône de couleur) : tous les composants de la protection ou certains d'entre eux fonctionnent ;

(icône noire et blanche) : tous les composants de la protection sont désactivés.

Accès au menu contextuel et aux fenêtres de l'application.

L'icône permet d'ouvrir le menu contextuel (à la page 32) (bouton droit de la souris) et la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 33) (bouton gauche de la souris).

L'icône apparaît dans la barre des tâches de Microsoft Windows lorsque des infos sont émises par Kaspersky Lab. La fenêtre Kiosque d'informations (cf. section "Kiosque d'informations" à la page 37) s'ouvre d'un double-clique sur cette icône.

MENU CONTEXTUEL

Le menu contextuel permet d'exécuter rapidement plusieurs actions sur l'application.

Le menu de Kaspersky Anti-Virus contient les points suivants :

- **Gestionnaire des tâches** : ouvre la fenêtre **Gestionnaire des tâches**.
- **Mise à jour** : lance le processus de mise à jour des bases et des modules de l'application.
- **Clavier virtuel** : affiche le clavier virtuel.
- **Kaspersky Anti-Virus** : ouvre la fenêtre principale de l'application.
- **Suspendre la protection/Restaurer la protection** : suspend temporairement/active le composant de la protection en temps réel. Cette option du menu n'a aucune influence sur la mise à jour de l'application, ni sur l'exécution de la recherche de virus.
- **Configuration** : ouvre la fenêtre de configuration de l'application.
- **A propos du programme** : ouvre la fenêtre contenant les informations relatives à l'application.
- **Infos** : ouvre la fenêtre du kiosque d'informations (cf. section "Kiosque d'informations" à la page 37). Cette option est visible uniquement lorsqu'il y a des informations non lues.
- **Terminer** : arrêt de Kaspersky Anti-Virus (si vous sélectionnez cette option, l'application sera déchargée de la mémoire vive de l'ordinateur).

Illustration 1. Menu contextuel

Si une tâche quelconque de recherche de virus ou de mise à jour est lancée quand vous ouvrez le menu contextuel, son nom apparaît dans le menu contextuel accompagné de la progression en pour cent. Après avoir sélectionné une tâche, vous pouvez passer à la fenêtre principale présentant le rapport avec les résultats détaillés de l'exécution.

Pour ouvrir le menu contextuel,

placez le curseur sur l'icône de l'application dans la zone de notification de la barre des tâches, puis cliquez avec le bouton droit de la souris.

Dans le système d'exploitation Microsoft Windows 7, l'icône de l'application est dissimulée par défaut. Pour utiliser l'application, vous pouvez l'afficher (cf. la documentation du système d'exploitation).

FENETRE PRINCIPALE DE KASPERSKY ANTI-VIRUS

La fenêtre principale de l'application reprend les éléments de l'interface qui permettent d'accéder à l'ensemble des fonctions principales de l'application.

La fenêtre principale est scindée en deux parties :

- La partie supérieure de la fenêtre contient les informations sur l'état de protection de votre ordinateur.

Illustration 2. Partie supérieure de la fenêtre principale

- La partie inférieure de la fenêtre permet d'accéder rapidement aux fonctions principales de l'application (par exemple, exécution des tâches d'analyse, mise à jour des bases et des modules de l'application).

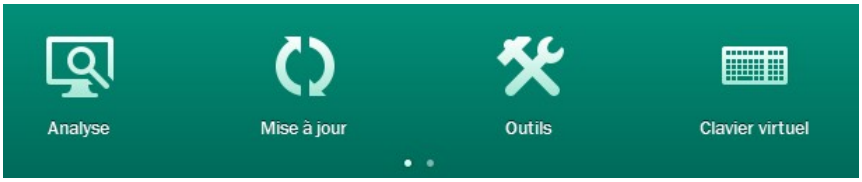

Illustration 3. Partie inférieure de la fenêtre principale

Lorsque vous sélectionnez une des sections dans la partie inférieure de la fenêtre, une fenêtre de la fonction correspondante de l'application s'ouvre. Vous pouvez revenir au choix des fonctions en cliquant sur le bouton **Précédent** en haut à gauche de la fenêtre.

Vous pouvez également cliquer sur les boutons et les liens suivants :

- **Cloud Protection** : passage aux informations sur Kaspersky Security Network (cf. page 129).
- **Configuration** : ouvre la fenêtre de configuration des paramètres de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 35).
- **Rapports** : passage aux rapports sur le fonctionnement de l'application.
- **Infos** : affiche les dernières nouvelles dans la fenêtre du kiosque d'informations (cf. section "Kiosque d'informations" à la page 37). Le lien apparaît après que l'application a reçu les informations.

- **Aide** : ouvre le système d'aide de Kaspersky Anti-Virus.
- **Mon Espace Personnel** : ouvre l'espace personnel de l'utilisateur sur le site web du service d'assistance technique.
- **Assistance technique** : ouvre la fenêtre contenant les informations relatives au système et les liens vers les sources d'informations de Kaspersky Lab (site du support technique, forum).
- **Gestionnaire de licences** : passe à l'activation de Kaspersky Anti-Virus et au renouvellement de la licence.

Vous pouvez ouvrir la fenêtre principale de l'application par un des moyens suivants :

- En cliquant sur le bouton gauche de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches.

  Dans le système d'exploitation Microsoft Windows 7, l'icône de l'application est dissimulée par défaut. Pour utiliser l'application, vous pouvez l'afficher (cf. la documentation du système d'exploitation).

- Sélectionnez l'option **Kaspersky Anti-Virus** dans le menu contextuel (cf. section "Menu contextuel" à la page 32).
- Cliquez sur l'icône de Kaspersky Anti-Virus, située au centre de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

FENETRE DE NOTIFICATION ET MESSAGES CONTEXTUELS

Kaspersky Anti-Virus vous signale les événements importants survenus pendant son fonctionnement à l'aide des *fenêtres de notification* et des *messages contextuels* qui apparaissent au-dessus de l'icône de l'application dans la zone de notification de la barre des tâches.

La fenêtre de notification de Kaspersky Anti-Virus s'affiche quand plusieurs actions sont possibles en rapport avec l'événement : par exemple, en cas de découverte d'un objet malveillant, vous pouvez bloquer l'accès à celui-ci, le supprimer ou tenter de le réparer. L'application vous propose de choisir parmi plusieurs options. La fenêtre de notification disparaît une fois que vous avez sélectionné une des actions proposées.

Illustration 4. Fenêtre notifications

Les messages contextuels de Kaspersky Anti-Virus s'affichent pour signaler des événements qui ne nécessitent pas obligatoirement une intervention. Certains messages contextuels contiennent des liens qui permettent d'exécuter l'action proposée (par exemple, lancer la mise à jour des bases ou activer l'application). Les messages contextuels disparaissent automatiquement de l'écran après l'affichage.

Illustration 5. Message contextuel

Les messages contextuels et les notifications sont répartis en trois catégories en fonction de l'importance de l'événement du point de vue de la protection de l'ordinateur :

- Critiques : signalent des événements d'une importance capitale pour assurer la protection de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Fenêtre des notifications et des messages contextuels critiques : en rouge.

- Importants : signalent des événements potentiellement importants pour assurer la protection de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Fenêtre des notifications et des messages contextuels importants : en jaune.

- Informatifs : signalent des événements qui ne sont pas critiques pour assurer la protection de l'ordinateur. Fenêtre des notifications et des messages contextuels informatifs : en vert.

FENETRE DE CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de Kaspersky Anti-Virus (ci-après aussi "fenêtre de configuration") permet de configurer les paramètres de fonctionnement de l'application dans son ensemble, de composants distincts de la protection, de l'analyse et de la mise à jour et d'exécuter d'autres tâches de configuration étendue (cf. section Configuration étendue de l'application à la page 63).

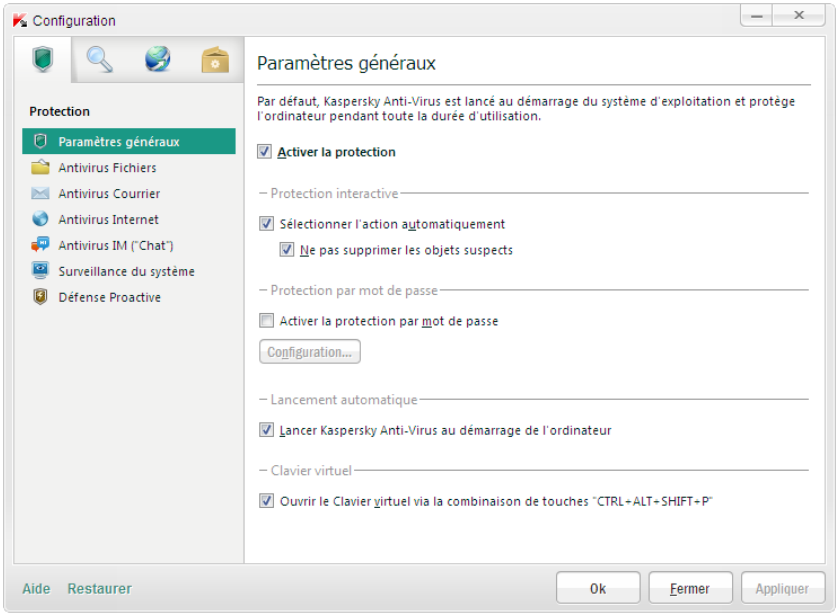

Illustration 6. Fenêtre de configuration des paramètres de l'application

La fenêtre de configuration contient deux parties :

- La partie gauche de la fenêtre permet de sélectionner le composant de l'application, la tâche ou tout autre élément qu'il faut configurer ;
- La partie droite de la fenêtre contient les éléments d'administration à l'aide desquels il est possible de configurer le fonctionnement des éléments choisis dans la partie gauche de la fenêtre.

Les composants, les tâches et autres éléments dans la partie gauche sont regroupés en section :

– **Protection** ;

– **Analyse de l'ordinateur** ;

– **Mise à jour** ;

– **Paramètres avancés**.

Vous pouvez ouvrir la fenêtre de configuration par un des moyens suivants :

- Passez au lien **Configuration** dans la partie supérieure de la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 33) ;
- Sélectionnez l'option **Configuration** dans le menu contextuel de l'application (cf. section "Menu contextuel" à la page 32) ;
- Cliquez sur le bouton avec l'icône **Configuration** dans l'interface de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7). Il faut associer la fonction d'ouverture de la fenêtre de configuration à ce bouton (cf. section "Utilisation de Kaspersky Gadget" à la page 61).

KASPERSKY GADGET

Si vous utilisez Kaspersky Anti-Virus sur un ordinateur tournant sous le système d'exploitation Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez utiliser Kaspersky Gadget (ci-après *gadget*). Kaspersky Gadget permet d'accéder rapidement aux fonctions principales de l'application (par exemple, indication de l'état de la protection de l'ordinateur, analyse des objets, consultation des rapports sur le fonctionnement de l'application).

Le gadget apparaît automatiquement sur le Bureau après l'installation de Kaspersky Anti-Virus sur un ordinateur fonctionnant sous Microsoft Windows 7. Après l'installation de l'application sur un ordinateur fonctionnant sous Microsoft Windows Vista, le gadget devra être ajouté manuellement au Volet Windows de Microsoft Windows (cf. la documentation du système d'exploitation).

Illustration 7. Kaspersky Gadget

KIOSQUE D'INFORMATIONS

Grâce au *kiosque d'informations*, Kaspersky Lab vous informe régulièrement des événements importants qui concernent Kaspersky Anti-Virus en particulier et la protection contre les menaces informatiques en général.

L'application vous signalera l'existence de nouvelles informations à l'aide de l'icône dans la zone de notification de la barre des tâches (cf. ci-dessous) et à l'aide du message contextuel. Les informations sur le nombre d'événements non lues apparaissent également dans la fenêtre principale de l'application. L'icône des informations apparaît dans l'interface du gadget de Kaspersky Anti-Virus.

Vous pouvez lire les nouvelles par un des moyens suivants :

- Via un clic sur l'icône  dans la zone de notification de la barre des tâches ;
- Via le lien **Lire les nouvelles** dans la fenêtre contextuelle présentant l'information ;
- Via le lien **Infos** dans la fenêtre principale de l'application ;
- Via l'icône qui apparaît au milieu du gadget quand une info est disponible (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

Les méthodes citées pour ouvrir le kiosque d'informations sont disponibles uniquement lorsqu'il y a des informations non lues.

Si vous voulez recevoir des informations, vous pouvez activer l'envoi des informations.

LANCEMENT ET ARRET DE L'APPLICATION

Cette section explique comment lancer et comment arrêter l'application.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DU LANCEMENT AUTOMATIQUE

Dans ce cas-ci, le lancement automatique de l'application signifie le lancement de Kaspersky Anti-Virus sans aucune intervention de votre part, directement après le démarrage du système d'exploitation. Ce mode de lancement est activé par défaut.

Pour activer ou désactiver le lancement automatique de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Paramètres généraux**.
3. Pour désactiver le lancement automatique de l'application, dans le groupe **Lancement automatique** de la partie droite de la fenêtre, décochez la case **Lancer Kaspersky Anti-Virus au démarrage de l'ordinateur**. Pour activer le lancement automatique de l'application, cochez cette case.

LANCEMENT ET ARRET MANUEL DU FONCTIONNEMENT DE L'APPLICATION

Kaspersky Lab déconseille d'arrêter Kaspersky Anti-Virus car, dans ce cas, la protection de l'ordinateur et des données personnelles qu'il contient seront menacées. Il est conseillé de suspendre temporairement la protection de l'ordinateur sans arrêter l'application.

Il faut lancer Kaspersky Anti-Virus manuellement uniquement si vous avez désactivé le lancement automatique de l'application (cf. section "Activation et désactivation du lancement automatique" à la page 38).

Pour lancer l'application manuellement,

dans le menu **Démarrer**, sélectionnez l'option **Applications → Kaspersky Anti-Virus 2012 → Kaspersky Anti-Virus 2012**.

Pour quitter l'application,

cliquez sur le bouton droit de la souis pour ouvrir le menu contextuel de l'icône de l'application, située dans la zone des notifications de la barre des tâches et sélectionnez dans le menu l'option **Terminer**.

Dans le système d'exploitation Microsoft Windows 7, l'icône de l'application est dissimulée par défaut. Pour utiliser l'application, vous pouvez l'afficher (cf. la documentation du système d'exploitation).

ADMINISTRATION DE LA PROTECTION DE L'ORDINATEUR

Cette section explique comment déterminer la présence de menaces contre la sécurité de l'ordinateur et comment configurer le niveau de protection. Vous apprendrez comment activer ou désactiver la protection et comment la suspendre temporairement pendant l'utilisation de l'application.

DANS CETTE SECTION

DIAGNOSTIC ET SUPPRESSION DES PROBLEMES DANS LA PROTECTION DE L'ORDINATEUR

L'indicateur, situé dans la partie gauche de la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 33), signale les problèmes qui pourraient survenir dans la protection de l'ordinateur. La couleur de l'indicateur (représente l'image du moniteur) change en fonction de l'état de la protection de l'ordinateur : le vert indique que l'ordinateur est protégé, le jaune signale un problème dans la protection et le rouge indique une menace sérieuse pour la sécurité de l'ordinateur.

Illustration 8. Indicateur d'état de la protection

Il est conseillé d'éliminer immédiatement les problèmes et les menaces sur la sécurité.

En cliquant sur l'indicateur dans la fenêtre principale de l'application, vous pouvez ouvrir la fenêtre **Problèmes de sécurité** (cf. ill. ci-après) qui affiche des informations détaillées sur l'état de la protection de l'ordinateur et qui propose diverses solutions pour supprimer les problèmes et les menaces.

Illustration 9. Fenêtre Problèmes de sécurité

Les problèmes dans la protection sont regroupés selon les catégories auxquelles ils appartiennent. Des actions que vous pouvez exécuter sont proposées à titre de résolution de chaque problème.

ACTIVATION ET DESACTIVATION DE LA PROTECTION

Kaspersky Anti-Virus est lancé par défaut au démarrage du système d'exploitation et protège votre ordinateur pendant la session. Tous les composants de la protection sont activés.

Vous pouvez désactiver la protection en temps réel offerte par Kaspersky Anti-Virus complètement ou partiellement.

Kaspersky Lab déconseille de désactiver la protection car cela pourrait entraîner l'infection de l'ordinateur et la perte de données. Il est recommandé de suspendre la protection pendant la durée requise (cf. section "Suspension et lancement de la protection" à la page 41).

Les indices suivants signalent la suspension ou la désactivation de la protection :

- L'icône de l'application dans la zone de notification de la barre des tâches est gris (cf. section "Icône dans la zone de notification" à la page 31) ;
- Couleur rouge de l'indicateur de sécurité dans la partie supérieure de la fenêtre principale de l'application.

La désactivation ou suspension du fonctionnement des composants de la protection n'a pas d'influence sur la recherche de virus et la mise à jour de Kaspersky Anti-Virus.

Il est possible d'activer ou de désactiver des composants de l'application depuis la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 35).

Pour désactiver ou activer complètement la protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Paramètres généraux**.
3. Décochez la case **Activer la protection** s'il faut désactiver la protection. Cochez cette case s'il faut activer la protection.

Pour activer ou désactiver le composant de la protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant qu'il faut activer ou désactiver.
3. Dans la partie droite de la fenêtre, décochez la case **Activer <nom du composant>** s'il faut désactiver le composant. Cochez cette case s'il faut activer le composant.

SUSPENSION ET LANCEMENT DE LA PROTECTION

La suspension de la protection signifie la désactivation de tous ses composants pour un certain temps.

Les indices suivants signalent la suspension ou la désactivation de la protection :

- L'icône de l'application dans la zone de notification de la barre des tâches est grise (cf. section "Icône dans la zone de notification" à la page 31) ;
- Couleur rouge de l'indicateur de sécurité dans la partie supérieure de la fenêtre principale de l'application.

Dans ce cas, la protection est envisagée dans le contexte des composants de la protection. La désactivation ou suspension du fonctionnement des composants de la protection n'a pas d'influence sur la recherche de virus et la mise à jour de Kaspersky Anti-Virus.

Si des connexions de réseau étaient ouvertes au moment de la suspension de la protection, un message sur l'interruption de celles-ci sera affiché.

Sur un ordinateur fonctionnant sous Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez suspendre la protection à l'aide du Kaspersky Gadget. Pour ce faire, il faut désigner une fonction de suspension de la protection pour un ou plusieurs boutons (cf. section "Utilisation de Kaspersky Gadget" à la page 61).

Pour suspendre la protection de l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre **Suspension de la protection** d'une des manières suivantes :
   - Sélectionnez l'option **Suspendre la protection** dans le menu contextuel de l'icône de l'application (cf. section "Menu contextuel" à la page 32) ;
   - Cliquez sur le bouton avec l'icône **Suspendre la protection** dans l'interface de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).
2. Dans la fenêtre **Suspension de la protection** sélectionnez la durée à l'issue de laquelle la protection sera à nouveau activée :
   - **Suspendre à l'heure indiquée** : la protection sera activée à l'issue de l'intervalle défini dans la liste déroulante ci-dessous.

- **Suspendre jusqu'au redémarrage** : la protection sera activée après le redémarrage de l'application ou du système d'exploitation (si le lancement automatique de l'application est activé (cf. section "Activation et désactivation du lancement automatique" à la page 38)).

- **Reprendre manuellement** : la protection sera activée lorsque vous déciderez de la rétablir (cf. ci-après).

Pour reprendre la protection de l'ordinateur,

sélectionnez l'option **Restaurer la protection** dans le menu contextuel de l'icône de l'application (cf. section "Menu contextuel" à la page 32).

Vous pouvez rétablir la protection de l'ordinateur de cette façon non seulement lorsque l'option **Reprendre manuellement** a été choisie pour la suspension, mais également en cas de sélection des options **Suspendre à l'heure indiquée** ou **Suspendre jusqu'au redémarrage**.

RESOLUTION DES PROBLEMES TYPES

Cette section contient des informations sur l'exécution des principales tâches liées à la protection de l'ordinateur à l'aide de l'application.

DANS CETTE SECTION

PROCEDURE D'ACTIVATION DE L'APPLICATION

L'*activation* est une procédure qui correspond à insérer un code dans le logiciel Kaspersky Lab afin d'en activer sa licence. Cette licence donne le droit d'utiliser la version commerciale de l'application pendant la durée de validité de la licence.

Si vous n'avez pas activé l'application pendant l'installation, vous pouvez le faire plus tard. Les notifications de Kaspersky Anti-Virus dans la zone de notifications de la barre des tâches vous rappelleront qu'il faut activer l'application.

Pour démarrer l'Assistant d'activation de Kaspersky Anti-Virus, exécutez une des actions suivantes :

- Passez au lien **Veuillez activer l'application** dans la fenêtre de notification de Kaspersky Anti-Virus dans la zone de notifications de la barre des tâches.

- Cliquez sur le lien **Saisissez le code d'activation**, situé dans la partie inférieure de la fenêtre principale de l'application. Dans la fenêtre **Gestionnaire de licences** qui s'ouvre, cliquez sur le bouton **Activer l'application**.

Lorsque l'Assistant d'activation de l'application fonctionne, certains paramètres doivent être indiqués.

Etape 1. Saisie du code d'activation

Saisissez le code d'activation dans le champ correspondant, puis cliquez sur **Suivant**.

Etape 2. Demande d'activation

Si la requête sur l'activation réussit, l'Assistant passe automatiquement à l'étape suivante.

Etape 3. Saisie des données d'enregistrement

L'enregistrement de l'utilisateur est nécessaire pour qu'il puisse s'adresser ultérieurement au support technique. Les utilisateurs non enregistrés bénéficient d'une assistance minimum.

Saisissez vos données pour l'enregistrement, puis cliquez sur le bouton **Suivant**.

Etape 4. Activation

Si l'activation de l'application a réussi, l'Assistant passe automatiquement à la fenêtre suivante.

Etape 5. Fin de l'Assistant

Cette fenêtre de l'Assistant reprend les informations sur les résultats de l'activation : type de licence utilisée et date de fin de validité de la licence.

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

PROCEDURE D'ACHAT OU DE RENOUVELLEMENT D'UNE LICENCE

Si vous avez installé Kaspersky Anti-Virus sans licence, vous pourrez acheter celle-ci après l'installation de l'application. A l'achat d'une licence, vous recevez le code requis pour activer l'application (cf. section "Procédure d'activation de l'application" à la page 43).

Quand la durée de validité de la licence approche de son échéance, vous pouvez la renouveler. Vous pouvez acheter une nouvelle licence sans attendre l'expiration du code d'activation en utilisation. Pour ce faire, l'ajout du code d'activation de réserve est requis. A l'issue de la période de validité de la licence utilisée, Kaspersky Anti-Virus active automatiquement le code d'activation de réserve.

Pour acheter une licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Le lien **Gestionnaire de licences**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Gestionnaire de licences**.

3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Acheter le code d'activation**.

   La page de la boutique en ligne où vous pouvez acheter la licence s'ouvre.

Pour ajouter un code d'activation de réserve, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Gestionnaire de licences**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Gestionnaire de licences**.

   La fenêtre **Gestion des licences** s'ouvre.

3. Dans la fenêtre ouverte dans le groupe **Code d'activation de réserve**, cliquez sur le bouton **Saisir le code d'activation**.

   L'Assistant d'activation de l'application s'ouvre.

4. Saisissez le code d'activation dans les champs correspondant, puis cliquez sur **Suivant**.

   Kaspersky Anti-Virus envoie les données au serveur d'activation pour vérification. Si la vérification réussit, l'Assistant passe automatiquement à l'étape suivante.

5. Sélectionnez l'option **Utiliser en tant que code de réserve**, puis cliquez sur le bouton **Suivant**.
6. A la fin de l'Assistant, cliquez sur **Terminer**.

QUE FAIRE EN CAS D'AFFICHAGE DE NOTIFICATIONS

Les notifications de l'application qui apparaissent dans la zone de notification de la barre des tâches signalent les événements survenus pendant l'utilisation de l'application et qui requièrent votre attention. En fonction de la gravité de l'événement, les notifications peuvent appartenir aux catégories suivantes :

- Critiques : signalent des événements d'une importance capitale pour assurer la protection de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Fenêtre des notifications et des messages contextuels critiques : en rouge.
- Importants : signalent des événements potentiellement importants pour assurer la protection de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Fenêtre des notifications et des messages contextuels importants : en jaune.
- Informatifs : signalent des événements qui ne sont pas critiques pour assurer la protection de l'ordinateur. Fenêtre des notifications et des messages contextuels informatifs : en vert.

Quand un tel message apparaît, il faut sélectionner une des actions proposées dans la notification. La version optimale, à savoir celle recommandée par les experts de Kaspersky Lab, est choisie par défaut.

PROCEDURE DE MISE A JOUR DES BASES ET DES MODULES DE L'APPLICATION

Kaspersky Anti-Virus vérifie automatiquement la présence des mises à jour sur les serveurs de mises à jour de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Anti-Virus les télécharge et les installe en arrière-plan. Vous pouvez lancer à la main la mise à jour de Kaspersky Anti-Virus à tout moment.

Le téléchargement des mises à jour depuis les serveurs de Kaspersky Lab requiert une connexion Internet.

- *Pour lancer la mise à jour depuis le menu contextuel,*

  sélectionnez l'option **Mise à jour** dans le menu contextuel de l'icône de l'application.

- *Pour lancer la mise à jour depuis la fenêtre principale de l'application, procédez comme suit :*

  1. Ouvrez la la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Mise à jour**.

  2. Dans la fenêtre **Mise à jour** qui s'ouvre, cliquez sur le bouton **Mettre à jour**.

PROCEDURE D'ANALYSE DES SECTEURS IMPORTANTS DE L'ORDINATEUR

L'analyse rapide désigne l'analyse des objets suivants :

- objets chargés au démarrage du système d'exploitation ;
- mémoire système ;
- des secteurs d'amorçage du disque ;
- des objets ajoutés par l'utilisateur (cf. section "Composition de la liste des objets à analyser" à la page 68).

Vous pouvez lancer une analyse des zones importantes d'une des méthodes suivantes :

- via un raccourci créé (cf. page 73) au préalable ;
- depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 33).

- *Pour lancer l'analyse via un raccourci, procédez comme suit :*

  1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier où vous avez créé le raccourci.

  2. Double-cliquez sur le raccourci pour lancer l'analyse.

- *Pour lancer l'analyse depuis la fenêtre principale de l'application, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.

  2. Dans la fenêtre ouverte **Analyse** dans le groupe **Analyse rapide**, cliquez sur le bouton  .

PROCEDURE DE RECHERCHE DE VIRUS DANS UN FICHIER, UN DOSSIER, UN DISQUE OU UN AUTRE OBJET

Pour analyser un objet distinct, utilisez une des méthodes suivantes :

- Via le menu contextuel de l'objet ;
- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 33) ;

- Via le gadget Kaspersky Anti-Virus (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

Pour lancer la recherche d'éventuels virus depuis le menu contextuel de l'objet, procédez comme suit :

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier contenant l'objet à analyser.

2. Ouvrez le menu contextuel de l'objet en cliquant avec le bouton droit de la souris (cf. ill. ci-après) et sélectionnez l'option **Rechercher d'éventuels virus**.

   La progression et le résultat d'exécution de la tâche sont illustrés dans la fenêtre **Gestionnaire des tâches**.

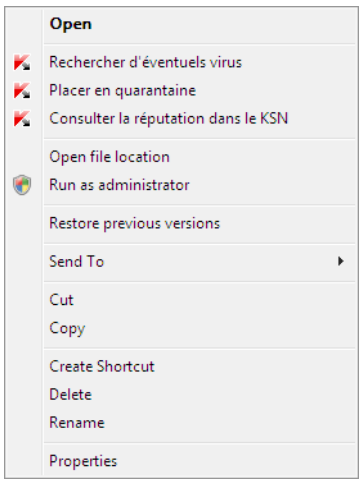

Illustration 10. Menu contextuel de l'objet dans Microsoft Windows

Pour lancer la recherche d'éventuels virus dans un objet depuis la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.

2. Désignez l'objet à analyser d'une des méthodes suivantes :

   - Cliquez sur le lien **désignez** situé dans la partie inférieure droite de la fenêtre pour ouvrir la fenêtre **Analyse personnalisée**, puis cochez les cases en regard des dossiers et des disques à analyser.

     Si l'objet à analyser ne figure pas dans la liste, procédez comme suit :

     a. Cliquez sur le bouton **Ajouter**.

     b. Dans la fenêtre ouverte **Sélection de l'objet à analyser**, sélectionnez l'objet à analyser.

   - Faites glisser l'objet à analyser dans la zone de la fenêtre principale prévue à cet effet (cf. ill. ci-dessous).

   Le processus d'exécution de la tâche apparaîtra dans la fenêtre ouverte **Gestionnaire des tâches**.

Illustration 11. Zone de la fenêtre Analyse sur laquelle il faut déposer l'objet à analyser

Pour rechercher la présence éventuelle de virus à l'aide du gadget,

faites glisser l'objet sur le gadget.

Le processus d'exécution de la tâche apparaîtra dans la fenêtre **Gestionnaire des tâches**.

PROCEDURE D'EXECUTION D'UNE ANALYSE COMPLETE DE L'ORDINATEUR

Vous pouvez lancer l'analyse complète de l'ordinateur d'une des méthodes suivantes :

- via un raccourci créé (cf. page 73) au préalable ;
- depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 33).

Pour lancer l'analyse complète via un raccourci, procédez comme suit :

1. Ouvrez l'Assistant de Microsoft Windows et accédez au dossier où vous avez créé le raccourci.
2. Double-cliquez sur le raccourci pour lancer l'analyse.

Pour lancer l'analyse complète depuis la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.
2. Dans la fenêtre ouverte **Analyse** dans le groupe **Analyse complète**, cliquez sur le bouton .

PROCEDURE DE RECHERCHE DE VULNERABILITES SUR L'ORDINATEUR

Une *vulnérabilité* est un endroit non protégé dans le code que des individus malintentionnés peuvent utiliser à leur fin, par exemple copier les données utilisées par l'application au code non protégé. La recherche de vulnérabilités potentielles sur votre ordinateur permet d'identifier les "points faibles" de la protection de votre ordinateur. Il est conseillé de supprimer les vulnérabilités découvertes.

Vous pouvez lancer la recherche de vulnérabilités d'une des manières suivantes :

- depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 33) ;
- via un raccourci créé (cf. page 73) au préalable.

Pour lancer une tâche à l'aide d'un raccourci, procédez comme suit :

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier où vous avez créé le raccourci.
2. Double-cliquez sur le raccourci pour lancer la tâche de recherche de vulnérabilités.

Pour lancer la tâche depuis la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.
2. Dans la fenêtre ouverte **Analyse** dans le groupe **Recherche de Vulnérabilités**, cliquez sur le bouton .

PROCEDURE DE PROTECTION DES DONNEES PERSONNELLES CONTRE LE VOL

Kaspersky Anti-Virus permet de protéger les données personnelles suivantes contre le vol :

- Mots de passe, noms d'utilisateur et autres données d'enregistrement ;
- Numéros de compte et de cartes de crédit.

Kaspersky Anti-Virus reprend des composants et des outils suivants qui permettent de protéger vos données personnelles :

- Anti-Phishing. Protège contre le vol des données, en utilisant l'hameçonnage (phishing).
- Clavier virtuel. Evite l'interception des données saisies à l'aide du clavier.

DANS CETTE SECTION

PROTECTION CONTRE L'HAMEÇONNAGE (PHISHING)

L'Anti-Phishing, inclus dans l'Antivirus Internet et l'Antivirus IM, garantit la protection contre l'hameçonnage (phishing). Kaspersky Lab recommande d'activer l'analyse sur l'hameçonnage (phishing) lors du fonctionnement de tous les composants de la protection.

Pour activer la protection contre l'hameçonnage (phishing) lors du fonctionnement de l'Antivirus Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. La fenêtre **Antivirus Internet** s'ouvre.
5. Dans la fenêtre ouverte sous l'onglet **Général**, dans le groupe **Analyse des liens**, cochez la case **Vérifier si les pages appartiennent à un site d'hameçonnage (phishing)**.

Pour activer la protection contre l'hameçonnage (phishing) lors du fonctionnement de l'Antivirus IM, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
3. Cochez la case **Analyser les liens selon la base des URL d'hameçonnage (phishing)** dans le groupe **Méthodes d'analyse** de la partie droite de la fenêtre.

PROTECTION CONTRE L'INTERCEPTION DES DONNEES A L'AIDE D'UN ENREGISTREUR DE FRAPPES (KEYLOGGER)

Au cours de l'utilisation d'Internet, il arrive souvent qu'il faille saisir des données personnelles ou un nom d'utilisateur et un mot de passe. Ceci se produit par exemple lors de l'ouverture d'une session sur un site web, lors de l'achat dans une boutique en ligne ou en cas d'utilisation d'un service de transactions bancaires en ligne.

Le risque existe que ces données soient interceptées à l'aide d'outils d'interception ou d'enregistreurs de frappes.

Le clavier virtuel permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.

Le clavier virtuel ne peut protéger vos données si le site web nécessitant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus malintentionnés.

De nombreux logiciels espions peuvent réaliser des captures d'écran qui sont transmises automatiquement à l'individu malintentionné pour analyse et récupération des données personnelles de l'utilisateur. Le clavier virtuel protège les données personnelles saisies contre l'interception par capture d'écran.

Le clavier virtuel protège contre l'interception des données personnelles uniquement avec les navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome.

Le clavier virtuel possède les particularités suivantes :

- Il faut appuyer sur les touches du clavier à l'aide de la souris.
- A la différence du clavier ordinaire, le clavier virtuel ne vous permet pas d'appuyer sur plusieurs touches en même temps. Par conséquent, si vous souhaitez utiliser une combinaison de touches (par exemple, **ALT+F4**), il faut d'abord appuyer sur la première touche (par exemple **ALT**), puis sur la deuxième (par exemple **F4**), puis à nouveau sur la première. La deuxième pression sur la première touche équivaut au relâchement des deux touches sur le clavier.
- Sur le clavier virtuel, vous pouvez changer la langue de saisie à l'aide de la combinaison de touches **CTRL+SHIFT** (dans ce cas, il faut appuyer sur la touche **SHIFT** avec le bouton droit de la souris) ou **CTRL+LEFT ALT** (cliquez sur la touche **LEFT ALT** avec le bouton droit de la souris), en fonction des paramètres définis.

Les méthodes suivantes s'offrent à vous pour ouvrir le clavier virtuel :

- Depuis le menu contextuel de l'application ;
- Au départ de la fenêtre principale de l'application ;
- Au départ du navigateur Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome ;
- À l'aide d'une combinaison de touches.

Pour ouvrir le clavier virtuel depuis le menu contextuel de l'icône de l'application,

Sélectionnez l'option **Clavier virtuel** dans le menu contextuel de l'icône de l'application.

Pour ouvrir le clavier virtuel depuis la fenêtre principale de l'application,

sélectionnez la section Clavier virtuel dans la partie inférieure de la fenêtre principale de l'application **Clavier virtuel**.

Pour ouvrir le clavier virtuel depuis la fenêtre du navigateur,

Cliquez sur le bouton  **Clavier virtuel** dans la barre d'outils de Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome.

Pour ouvrir le clavier virtuel à l'aide du clavier physique,

utilisez la combinaison de touches **CTRL+ALT+SHIFT+P**.

QUE FAIRE SI VOUS PENSEZ QUE L'OBJET EST INFECTE PAR UN VIRUS

Si vous pensez que l'objet est infecté par un virus, analysez-le à l'aide de Kaspersky Anti-Virus (cf. section "Procédure d'analyse d'un objet distinct (fichier, dossier, disque)" à la page 46).

Si l'application, suite à l'analyse, signale que l'objet est sain, mais que vous pensez que ce n'est pas le cas, vous pouvez exécuter une des actions suivantes :

- Placer l'objet en *quarantaine*. Les objets placés en quarantaine ne constituent aucune menace pour votre ordinateur. Il se peut, après la mise à jour des bases, que Kaspersky Anti-Virus puisse identifier la menace et la supprimer.
- Envoyer l'objet au *Laboratoire d'étude des virus*. Les experts du laboratoire d'étude des virus étudieront l'objet pour voir s'il est vraiment infecté par un virus et ajouteront sur le champ la description du nouveau virus aux bases qui seront chargées par l'application lors de la mise à jour (cf. section "Procédure de mise à jour des bases et des modules de l'application" à la page 45).

Un fichier peut être placé en quarantaine de deux manières :

- à l'aide du bouton **Placer en quarantaine** dans la fenêtre **Quarantaine** ;
- via le menu contextuel du fichier.

Pour placer le fichier en quarantaine depuis la fenêtre Quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.
3. Sous l'onglet **Quarantaine**, cliquez sur le bouton **Placer en quarantaine**.
4. Dans la fenêtre qui s'ouvre, choisissez le fichier qu'il faut placer en quarantaine.

Pour placer un fichier en quarantaine à l'aide du menu contextuel, procédez comme suit :

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier contenant le fichier à mettre en quarantaine.
2. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Copier dans la quarantaine**.

Pour envoyer le fichier au laboratoire d'étude des virus, procédez comme suit :

1. Ouvrez la page d'envoi de requêtes au Laboratoire d'étude des virus (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr).
2. Suivez les instructions affichées sur la page pour envoyer votre demande.

QUE FAIRE SI VOUS PENSEZ QUE VOTRE ORDINATEUR EST INFECTE

Si vous pensez que, suite à l'activité des programmes malveillants ou aux erreurs de système, le système d'exploitation de votre ordinateur a été corrompu, utilisez l'*Assistant de restauration du système* qui élimine les traces de la présence d'objets malveillants dans le système. Les experts de Kaspersky Lab conseillent également de lancer l'Assistant après la réparation de l'ordinateur afin de confirmer que toutes les menaces et les dommages ont été supprimés.

L'Assistant de restauration vérifie la présence des modifications et des dégâts dans le système (par exemple, les modifications des extensions des fichiers, le bocage de l'environnement de réseau et du panneau de configuration). Les causes possibles des modifications et des dégâts sont : l'activité des programmes malveillants, la configuration incorrecte du système, les erreurs de système ou l'utilisation des applications d'optimisation du système qui ne fonctionnent pas correctement.

Après l'étude, l'Assistant analyse les informations recueillies afin d'identifier les dommages dans le système qui requièrent une intervention immédiate. La liste des actions à exécuter pour supprimer l'infection est générée sur la base des résultats de l'analyse. L'Assistant regroupe les actions en catégorie selon la gravité des problèmes identifiés.

Pour lancer l'Assistant de restauration du système, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 33).
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils**.
3. Dans la fenêtre ouverte dans le groupe **Restauration du système**, cliquez sur le bouton **Exécuter**.

   La fenêtre de l'Assistant de restauration du système s'ouvrira.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Etape 1. Lancement de la restauration du système

Assurez-vous que l'option **Rechercher les problèmes liés à l'activité d'un programme malveillant** a été sélectionnée dans la fenêtre de l'Assistant, puis cliquez sur le bouton **Suivant**.

Etape 2. Recherche des problèmes

L'Assistant recherche les problèmes et les dégâts potentiels qu'il faut supprimer. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 3. Sélection d'actions pour la résolution des problèmes

Tous les problèmes identifiés à l'étape précédente sont regroupés en fonction du danger qu'ils présentent. Pour chaque groupe de corruptions, les experts de Kaspersky Lab proposent un ensemble d'actions dont l'exécution contribuera à l'élimination des problèmes. Trois groupes d'actions ont été désignés :

- Les *actions vivement recommandées* permettent de supprimer les corruptions qui constituent un problème sérieux. Il est conseillé d'exécuter toutes les actions de ce groupe.
- Les *actions recommandées* visent à supprimer les corruptions qui peuvent présenter un danger potentiel. L'exécution des actions de ce groupe est également recommandée.
- Les *actions complémentaires* sont prévues pour supprimer les corruptions du système qui ne présentent actuellement aucun danger mais qui à l'avenir pourraient menacer la sécurité de l'ordinateur.

Pour voir les actions reprises dans le groupe, cliquez sur le signe **+** situé à gauche du nom du groupe.

Pour que l'Assistant réalise une action, cochez la case à gauche du nom de l'action. Toutes les actions recommandées et vivement recommandées sont exécutées par défaut. Si vous ne souhaitez pas exécuter une action quelconque, désélectionnez la case en regard de celle-ci.

Il est vivement déconseillé de décocher les cases sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.

Une fois que vous aurez sélectionné les actions pour l'Assistant, cliquez sur **Suivant**.

Etape 4. Suppression des problèmes

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des problèmes peut durer un certain temps. Une fois la suppression des problèmes terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 5. Fin de l'Assistant

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

PROCEDURE DE RESTAURATION D'UN FICHIER SUPPRIME OU REPARE PAR L'APPLICATION

Kaspersky Lab déconseille la restauration des fichiers supprimés ou réparés car ils peuvent constituer une menace pour votre ordinateur.

Si la restauration d'un fichier supprimé ou réparé s'impose, utilisez sa copie de sauvegarde créée par l'application lors de l'analyse.

Pour restaurer un fichier supprimé ou réparé par l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.
3. Sous l'onglet **Sauvegarde**, sélectionnez le fichier nécessaire dans la liste et cliquez sur le bouton **Restaurer**.

PROCEDURE DE CREATION DU DISQUE DE DEPANNAGE ET UTILISATION DE CELUI-CI

Après l'installation de Kaspersky Anti-Virus et après la première analyse de l'ordinateur, il est recommandé de créer le disque de dépannage.

Le disque de dépannage représente l'application Kaspersky Rescue Disk enregistrée sur le support amovible (CD ou périphérique USB).

A l'avenir, vous pourrez utiliser Kaspersky Rescue Disk pour analyser et réparer l'ordinateur infecté dont la réparation par n'importe quel autre moyen est impossible (par exemple, à l'aide d'un logiciel antivirus).

DANS CETTE SECTION

CREATION D'UN DISQUE DE DEPANNAGE

La création du disque de dépannage consiste à générer une image du disque (fichier au format ISO) avec la version actuelle de l'application Kaspersky Rescue Disk et son enregistrement sur le support amovible.

L'image du disque de départ peut être téléchargée du serveur de Kaspersky Lab ou copiée depuis une source locale.

Le disque de dépannage est créé à l'aide de l'*Assistant de création et d'enregistrement de Kaspersky Rescue Disk*. Le fichier de l'image rescuecd.iso créé par l'Assistant est enregistré sur le disque dur de l'ordinateur.

- Sous Microsoft Windows XP dans le dossier : Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Data\Rdisk\ ;
- Sous Microsoft Windows Vista et Microsoft Windows 7 dans le dossier : ProgramData\Kaspersky Lab\AVP12\Data\Rdisk\.

Pour créer un disque de dépannage, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils**.
3. Dans la fenêtre ouverte dans le groupe **Kaspersky Rescue Disk**, cliquez sur le bouton **Créer**.

   La fenêtre **Assistant de création de disque de dépannage** s'ouvrira.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Examinons en détails les étapes de l'Assistant.

Etape 1. Début de l'utilisation de l'Assistant. Recherche d'une image de disque existante

La première fenêtre de l'Assistant reprend les informations sur l'application Kaspersky Rescue Disk.

Si l'Assistant découvre un fichier d'image de disque dans le dossier prévu à cet effet (cf. ci-dessus), alors la case **Utiliser l'image existante** apparaît dans la première fenêtre. Cochez la case pour utiliser le fichier découvert en guise d'image source pour le disque et passez directement à l'étape **Mise à jour de l'image du disque** (cf. ci-après). Si vous ne voulez pas utiliser l'image du disque trouvée, décochez cette case. L'Assistant passera à la fenêtre **Sélection de la source de l'image du disque**.

Etape 2. Sélection de la source de l'image du disque

Si dans la fenêtre précédente de l'Assistant vous avez coché la case **Utiliser l'image existante**, alors cette étape n'est pas présentée.

Cette étape vous oblige à sélectionner une source de l'image du disque parmi les options proposées :

- Sélectionnez l'option **Copier l'image sur le disque local ou de réseau** si vous possédez déjà une image du disque de dépannage ou son image (fichier au format ISO) et qu'elle se trouve sur l'ordinateur ou sur une ressource du réseau local.

- Sélectionnez l'option **Télécharger l'image depuis les serveurs de Kaspersky Lab** si vous n'avez pas de fichier de l'image du disque de dépannage afin de le télécharger depuis le serveur de Kaspersky Lab (le fichier pèse environ 175 Mo).

Etape 3. Copie (téléchargement) de l'image du disque

Si dans la fenêtre précédente de l'Assistant vous avez coché la case **Utiliser l'image existante**, alors cette étape n'est pas présentée.

Si à l'étape précédente vous aviez choisi l'option **Copier l'image sur le disque local ou de réseau**, cliquez sur le bouton **Parcourir**. Après avoir indiqué le chemin d'accès au fichier, cliquez sur **Suivant**. La progression de la copie de l'image de disque est illustrée dans la fenêtre de l'Assistant.

Si à l'étape précédente vous aviez choisi l'option **Télécharger l'image depuis les serveurs de Kaspersky Lab**, alors la progression du téléchargement s'affichera directement.

Une fois que la copie ou le téléchargement de l'image de disque sera terminé, l'Assistant passera automatiquement à l'étape suivante.

Etape 4. Mise à jour du fichier de l'image du disque

La procédure de mise à jour du fichier de l'image du disque reprend les actions suivantes :

- La mise à jour des bases antivirus ;

- La mise à jour des fichiers de configuration.

Les fichiers de configuration déterminent la possibilité de charger l'ordinateur depuis le support amovible (par exemple, CD/DVD ou périphérique USB avec Kaspersky Rescue Disk) créé à l'aide de l'Assistant.

Lors de la mise à jour des bases antivirus, les bases obtenues suite à la mise à jour la plus récente de Kaspersky Anti-Virus sont utilisées. Si les bases sont dépassées, il est conseillé de réaliser une mise à jour, de relancer l'Assistant de création et d'enregistrement de Kaspersky Rescue Disk.

Pour lancer la mise à jour du fichier, cliquez sur **Suivant**. La fenêtre de l'Assistant illustrera la progression de la mise à jour.

Etape 5. Enregistrement de l'image du disque sur un support

Cette étape de l'Assistant vous informera que la création de l'image du disque a réussi et proposera d'enregistrer l'image du disque sur le support.

Désignez le support pour l'enregistrement de Kaspersky Rescue Disk :

- Pour enregistrer sur le CD/DVD, sélectionnez l'option **Enregistrer sur le CD/DVD** et indiquez le disque à enregistrer l'image du disque.

- Pour enregistrer sur le périphérique USB; sélectionnez l'option **Ecrire sur un périphérique USB** et indiquez le périphérique à enregistrer l'image du disque.

Kaspersky Lab déconseille d'enregistrer l'image de disque sur un périphérique qui n'est pas prévu exclusivement pour le stockage de données, comme un smartphone, un téléphone mobile, un ordinateur de poche ou un lecteur MP3. L'enregistrement de l'image de disque sur de tels appareils pourrait nuire au fonctionnement ultérieur de ceux-ci.

- Pour enregistrer sur le disque dur de votre ordinateur ou sur un autre ordinateur auquel vous avez l'accès par le réseau, sélectionnez l'option **Enregistrer l'image dans le fichier sur le disque local ou de réseau** et indiquez le dossier à enregistrer l'image du disque, et le nom du fichier au format ISO.

Etape 6. Fin de l'Assistant

Pour quitter l'Assistant, cliquez sur **Terminer**. Vous pouvez utiliser le disque de dépannage créé pour démarrer l'ordinateur (cf. page 56), si, suite à des actions des virus et des programmes malveillants, il n'est pas possible de démarrer l'ordinateur et de lancer Kaspersky Anti-Virus en mode normal.

DEMARRAGE DE L'ORDINATEUR A L'AIDE DU DISQUE DE DEPANNAGE

S'il est impossible de charger le système d'exploitation suite à une attaque de virus, utilisez le disque de dépannage.

Le chargement du système d'exploitation requiert le CD-/DVD- ou le périphérique USB contenant le programme Kaspersky Rescue Disk (cf. section "Création d'un disque de dépannage" à la page 54).

Le lancement de l'ordinateur depuis un support amovible n'est pas toujours possible. C'est le cas par exemple si l'ordinateur appartient à des anciennes générations. Avant d'éteindre l'ordinateur en vue de le redémarrer depuis un support amovible, vérifiez si cette option est prise en charge par l'ordinateur.

Pour démarrer l'ordinateur à l'aide du disque de dépannage, procédez comme suit :

1. Dans les paramètres BIOS, activez le chargement depuis un CD/DVD ou depuis un périphérique USB (pour obtenir de plus amples informations, consultez la documentation de la carte mère de votre ordinateur).
2. Introduisez le CD/DVD dans le lecteur de l'ordinateur infecté ou connectez le périphérique USB contenant l'application Kaspersky Rescue Disk.
3. Redémarrez l'ordinateur.

Pour en savoir plus sur l'utilisation du disque de dépannage, consultez le guide de l'utilisateur de Kaspersky Rescue Disk.

EMPLACEMENT DU RAPPORT SUR LE FONCTIONNEMENT DE L'APPLICATION

Kaspersky Anti-Virus crée un rapport sur le fonctionnement de chacun de ses composants. Ce rapport donne des données statistiques sur le fonctionnement de l'application (par exemple, nombre d'objets malveillants détectés et neutralisés pendant la période indiquée, nombre de fois que l'application a été actualisée, nombre de messages non sollicités détectés, etc.).

Si vous travaillez sur un ordinateur fonctionnant sous Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez ouvrir les rapports à l'aide du Kaspersky Gadget. Pour ce faire, Kaspersky Gadget doit être configuré de telle manière qu'un de ses boutons soit associé à la fonction d'ouverture de la fenêtre des rapports (cf. section "Utilisation de Kaspersky Gadget" à la page 61).

Pour consulter le rapport sur le fonctionnement du composant, procédez comme suit :

1. Ouvrez la fenêtre **Rapports** d'une des méthodes suivantes :
   - Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application ;
   - Cliquez sur le bouton avec l'icône **Rapports** dans l'interface de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

La fenêtre **Rapports** affiche les rapports sur l'activité de l'application sous la forme de schéma.

2. Pour consulter un rapport détaillé (par exemple un rapport sur chacun des composants de l'application), cliquez sur le bouton **Rapport détaillé** situé dans la partie inférieure de la fenêtre **Rapport**.

   La fenêtre **Rapport détaillé** s'ouvre. Elle présente les données sous forme d'un tableau. Pour faciliter la lecture du tableau, il est possible de regrouper les entrées du tableau selon différents critères.

PROCEDURE DE RESTAURATION DES PARAMETRES STANDARDS D'UTILISATION DE L'APPLICATION

A tout moment, vous pouvez restaurer les paramètres du fonctionnement de Kaspersky Anti-Virus recommandés par Kaspersky Lab. La restauration des paramètres s'opère à l'aide de l'*Assistant de configuration de l'application*.

A l'issue de l'utilisation de l'Assistant, le niveau de protection **Recommandé** sera sélectionné pour tous les composants de la protection. A la restauration du niveau de protection recommandé, vous pouvez enregistrer sélectivement les paramètres configurés auparavant pour les composants de l'application.

Pour restaurer les paramètres de fonctionnement standard de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Lancez l'Assistant de configuration de l'application d'une des manières suivantes :

   - Cliquez sur le lien **Restaurer** dans la partie inférieure de la fenêtre ;

   - Dans la partie gauche de la fenêtre, choisissez la section **Paramètres avancés**, sous-section **Administration des paramètres**, puis cliquez sur le bouton **Restaurer** dans le groupe **Restauration des paramètres standard**.

Examinons en détails les étapes de l'Assistant.

Etape 1. Début de l'utilisation de l'Assistant

Cliquez sur le bouton **Suivant** afin de poursuivre l'Assistant.

Etape 2. Restauration des paramètres

Cette fenêtre de l'Assistant reprend les composants de la protection de Kaspersky Anti-Virus dont les paramètres ont été modifiés par l'utilisateur. Si des paramètres uniques ont été définis pour un composant quelconque, ils figureront également dans la fenêtre.

Cochez la case en regard des paramètres à enregistrer, puis cliquez sur le bouton **Suivant**.

Etape 3. Fin de la restauration

Pour quitter l'Assistant, cliquez sur **Terminer**.

PROCEDURE DE TRANSFERT DES PARAMETRES DE L'APPLICATION DANS UNE VERSION DE KASPERSKY ANTI-VIRUS INSTALLEE SUR UN AUTRE ORDINATEUR

Après avoir configuré l'application, vous pouvez appliquer ses paramètres de fonctionnement à une version de Kaspersky Anti-Virus installée sur un autre ordinateur. L'application sur les deux ordinateurs sera configurée de la même manière. Cela est utile si vous avez installé Kaspersky Anti-Virus sur votre ordinateur chez vous et au bureau.

Les paramètres de fonctionnement de l'application sont enregistrés dans un fichier de configuration que vous pouvez transférer d'un ordinateur à l'autre.

Le transfert des données de Kaspersky Anti-Virus d'un ordinateur vers un autre s'effectue en trois étapes :

1. Enregistrement des paramètres de l'application dans le fichier de configuration.
2. Le transfert du fichier de configuration vers un autre ordinateur (par exemple, par courrier électronique ou via support amovible).
3. L'application des paramètres du fichier de configuration au programme installé sur l'autre ordinateur.

Pour exporter les paramètres actuels de fonctionnement de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Administration des paramètres**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Exporter**.
4. Saisissez le nom du fichier de configuration dans la fenêtre qui s'ouvre et précisez l'emplacement de la sauvegarde.
5. Cliquez sur le bouton **OK**.

Pour importer les paramètres de fonctionnement depuis le fichier de configuration, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Administration des paramètres**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Télécharger**.
4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier à utiliser pour importer les paramètres de Kaspersky Anti-Virus.
5. Cliquez sur le bouton **OK**.

COMMENT PASSER A KASPERSKY INTERNET SECURITY

Kaspersky Anti-Virus permet de passer à l'utilisation de l'application Kaspersky Internet Security sans le téléchargement complémentaire et l'installation du logiciel.

Kaspersky Internet Security est une application conçue pour une protection approfondie de votre ordinateur. Elle possède plusieurs possibilités complémentaires qui se réalisent à l'aide des modules et des fonctions suivants :

- Contrôle des Applications ;
- Contrôle Parental ;
- Pare-feu ;
- Prévention des intrusions ;
- Filtrage par géo localisation ;
- Blocage de l'accès aux sites dangereux ;
- Surveillance du réseau ;
- Anti-Spam ;
- Anti-bannière ;
- Suppression des traces d'activité ;
- Environnement protégé.

Vous pouvez temporairement basculer sur la version d'évaluation de Kaspersky Internet Security pour en savoir plus sur ses possibilités, ou de passer immédiatement avec la version commerciale de l'application.

Lors de l'utilisation de la licence avec l'abonnement, ainsi que lors du travail avec l'application dans certaines régions la permutation temporaire sur la version d'évaluation de Kaspersky Internet Security n'est pas prévue.

DANS CETTE SECTION

PERMUTATION SUR LA VERSION COMMERCIALE

Si vous voulez basculer sur la version commerciale de Kaspersky Internet Security, il vous faudra le code d'activation de la version commerciale de l'application à l'aide duquel vous pourrez l'activer (cf. section "Procédure d'activation de l'application" à la page 43).

Pour acheter un code d'activation pour Kaspersky Internet Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Offre de migration**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Acheter le code d'activation**.

Vous allez passer sur le site Web de la boutique en ligne où vous allez pouvoir acheter le code d'activation pour Kaspersky Internet Security.

Si vous avez acheté Kaspersky Anti-Virus dans certaines régions ou vous utilisez la licence avec l'abonnement, la section **Offre de migration** est absente dans la fenêtre principale.

PERMUTATION TEMPORAIRE SUR LA VERSION D'EVALUATION

Vous pouvez temporairement basculer sur la version d'évaluation de Kaspersky Internet Security pour évaluer ses possibilités. Si vous voulez, vous pouvez acheter une licence pour le travail permanent avec l'application.

Pour basculer temporairement sur Kaspersky Internet Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Offre de migration**.
3. Dans la fenêtre ouverte, cliquez sur le bouton **Version d'évaluation**.

   L'Assistant de configuration de l'application se lancera.

Si vous avez acheté Kaspersky Anti-Virus dans certaines régions ou vous utilisez la licence avec l'abonnement, la section **Offre de migration** est absente dans la fenêtre principale.

Lorsque l'Assistant de configuration de l'application fonctionne, certains paramètres doivent être indiqués.

Etape 1. Demande d'activation de la version d'évaluation de Kaspersky Internet Security

Si la requête sur l'activation de Kaspersky Internet Security réussit, l'Assistant passe automatiquement à l'étape suivante.

Etape 2. Début d'extension de la protection

A cette étape, l'Assistant affiche sur l'écran un message sur la disponibilité d'exécution de l'extension. Pour continuer le fonctionnement de l'Assistant, cliquez sur le bouton **Suivant**.

Etape 3. Suppression des applications incompatibles

A cette étape, l'Assistant vérifie la présence sur votre ordinateur des applications incompatibles avec Kaspersky Internet Security. Si ces applications n'existent pas, l'Assistant passe automatiquement à l'étape suivante. Si telles applications sont détectées, l'Assistant affichera leur liste dans la fenêtre et proposera de les supprimer.

Après la suppression des applications incompatibles, le redémarrage du système d'exploitation peut être requis. Après le redémarrage, l'Assistant sera automatiquement lancé et le processus d'extension de la protection sera poursuivi.

Etape 4. Offre de migration

Cette étape effectue la connexion des modules d'extension. Cela peut prendre un certain temps. Une fois le processus terminé, l'Assistant passe automatiquement à l'étape suivante.

Etape 5. Redémarrage de l'application

L'étape finale requiert le redémarrage de l'application. Pour ce faire, cliquez sur le bouton **Terminer** dans la fenêtre de l'Assistant.

Etape 6. Fin de l'activation

Après le redémarrage de l'application, l'Assistant sera lancé automatiquement. Lors de l'activation réussie de la version d'évaluation de Kaspersky Internet Security, la fenêtre de l'Assistant affiche les informations sur la durée d'utilisation de la version d'évaluation.

Etape 7. Analyse du système

Cette étape correspond à la collecte d'informations sur les applications reprises dans Microsoft Windows. Ces applications figurent dans la liste des applications de confiance et elles ne sont soumises à aucune restriction sur les actions qu'elles peuvent réaliser dans le système.

Une fois l'analyse terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 8. Fin de l'extension

Pour quitter l'Assistant, cliquez sur **Terminer**.

La deuxième permutation temporaire sur la version d'évaluation de Kaspersky Internet Security n'est pas prévue.

UTILISATION DE KASPERSKY GADGET

Si vous utilisez Kaspersky Anti-Virus sur un ordinateur tournant sous le système d'exploitation Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez utiliser Kaspersky Gadget (ci-après *gadget*). Le gadget apparaît automatiquement sur le Bureau après l'installation de Kaspersky Anti-Virus sur un ordinateur fonctionnant sous Microsoft Windows 7. Après l'installation de l'application sur un ordinateur fonctionnant sous Microsoft Windows Vista, le gadget devra être ajouté manuellement au Volet Windows de Microsoft Windows (cf. la documentation du système d'exploitation).

L'indicateur de couleur du gadget signale l'état de la protection de votre ordinateur de la même manière que l'indicateur situé dans la fenêtre principale de l'application (cf. section "Diagnostic et suppression des problèmes dans la protection de l'ordinateur" à la page 39). La couleur verte indique que l'ordinateur est protégé, la couleur jaune signale un problème dans la protection, la couleur rouge indique une menace sérieuse pour la sécurité de l'ordinateur. La couleur grise de l'indicateur indique que le fonctionnement de l'application a été arrêté.

Au cours de la mise à jour des bases et des modules de l'application, une icône d'un globe en rotation apparaît au milieu du gadget.

A l'aide du gadget, vous pouvez exécuter les actions suivantes :

- Restaurer le fonctionnement de l'application s'il a été suspendu ;
- Ouvrir le menu principal de l'application ;
- Rechercher la présence éventuelle de virus dans des objets en particuliers ;
- Ouvrir la fenêtre de consultation des nouvelles.

Vous pouvez aussi configurer les boutons du gadget pour exécuter les actions complémentaires :

- lancer la mise à jour ;
- modifier les paramètres de fonctionnement de l'application ;
- consulter les rapports de l'application ;
- suspendre la protection ;

- ouvrir le clavier virtuel ;
- ouvrir la fenêtre Gestionnaire des tâches.

Pour lancer l'application à l'aide du gadget,

cliquez sur l'icône **Activer** située au milieu du gadget.

Pour ouvrir la fenêtre principale de l'application à l'aide du gadget,

cliquez sur l'image du moniteur au milieu du gadget.

Pour rechercher la présence éventuelle de virus à l'aide du gadget,

faites glisser l'objet sur le gadget.

Le processus d'exécution de la tâche apparaîtra dans la fenêtre **Gestionnaire des tâches**.

Pour ouvrir la fenêtre de consultation des nouvelles à l'aide du gadget,

cliquez sur l'icône qui apparaît au milieu du gadget quand une info est disponible.

Pour configurer le gadget, procédez comme suit :

1. Ouvrez la fenêtre de configuration du gadget en cliquant sur l'icône qui apparaît dans le coin supérieur droit du gadget lorsque le curseur est placé sur celui-ci.
2. Dans les listes déroulantes qui correspondent aux boutons du gadget, sélectionnez les actions à exécuter lorsque vous cliquez sur les boutons du gadget.
3. Cliquez sur le bouton **OK**.

VERIFICATION DE LA REPUTATION DE L'APPLICATION

Kaspersky Anti-Virus permet de vérifier la réputation d'une application auprès des utilisateurs du monde entier.
La réputation de l'application reprend les indices suivants :

- nom de l'éditeur ;
- informations sur la signature numérique (disponible en présence de la signature numérique) ;
- informations sur le groupe dans lequel l'application a été placée ou par la majorité des utilisateurs de Kaspersky Security Network ;
- nombre d'utilisateurs de Kaspersky Security Network qui utilisent l'application (disponible si l'application est classée dans le groupe De confiance dans la base Kaspersky Security Network) ;
- heure à laquelle l'application est devenue connue dans Kaspersky Security Network ;
- pays dans lesquels l'application est la plus répandue.

Pour vérifier la réputation de l'application, à l'installation de Kaspersky Anti-Virus vous devez accepter la participation Kaspersky Security Network (cf. page 130).

Pour connaître la réputation d'une application,

ouvrez le menu contextuel du fichier exécutable de l'application et sélectionnez l'option **Consulter la réputation dans le KSN**.

CONFIGURATION ETENDUE DE L'APPLICATION

Cette section contient les informations complémentaires sur la configuration des paramètres de chaque composant de l'application.

DANS CETTE SECTION

PARAMETRES PRINCIPAUX DE LA PROTECTION

Dans la fenêtre de configuration de l'application, dans la sous-section **Paramètres généraux** de la section **Protection**, vous pouvez réaliser les opérations suivantes :

- désactiver tous les composants de la protection (cf. section "Activation et désactivation de la protection" à la page 40) ;

- sélectionner le mode de protection interactif ou automatique (cf. section "Sélection du mode de protection" à la page 64) ;
- limiter l'accès des utilisateurs à l'application à l'aide d'un mot de passe (cf. section "Restriction de l'accès à Kaspersky Anti-Virus" à la page 64) ;
- désactiver ou activer l'exécution automatique de l'application au démarrage du système d'exploitation (cf. section "Activation et désactivation du lancement automatique" à la page 38) ;
- activer une combinaison de touches non définie pour afficher le clavier virtuel (cf. section "Protection contre l'interception des données saisies au clavier" à la page 50).

DANS CETTE SECTION

RESTRICTION DE L'ACCES A KASPERSKY ANTI-VIRUS

Il se peut que l'ordinateur soit utilisé par plusieurs personnes possédant un niveau différent de maîtrise de l'informatique. L'accès illimité des utilisateurs à Kaspersky Anti-Virus et à ses paramètres peut entraîner une réduction du niveau de la protection de l'ordinateur dans son ensemble.

Pour limiter l'accès à l'application, vous pouvez définir un mot de passe et désigner les actions pour lesquelles il devra être saisi.

- modification des paramètres de fonctionnement de l'application ;
- arrêt de l'application ;
- suppression de l'application.

Utilisez avec prudence le mot de passe pour limiter l'accès à la suppression de l'application. Si vous oubliez le mot de passe, il sera difficile de supprimer l'application de l'ordinateur.

Pour limiter l'accès à Kaspersky Anti-Virus via un mot de passe, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Paramètres généraux**.
3. Dans la partie droite de la fenêtre, dans le groupe **Protection par mot de passe**, cochez la case **Activer la protection par mot de passe**, puis cliquez sur **Configuration**.
4. Dans la fenêtre **Protection par mot de passe** qui s'ouvre, saisissez le mot de passe et désignez les secteurs qui seront soumis à la restriction d'accès.

SELECTION DU MODE DE PROTECTION

Kaspersky Anti-Virus fonctionne par défaut dans le mode *automatique de la protection*. Dans ce mode, lors de l'apparition des événements dangereux, l'application applique automatiquement l'action recommandée par les experts de Kaspersky Lab. Vous pouvez installer un *mode de protection interactif*, pour que Kaspersky Anti-Virus vous informe sur tous les événements dangereux et suspects dans le système et offre la possibilité de prendre indépendamment la décision sur l'action proposée par l'application à appliquer.

Pour sélectionner le mode de protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez la sous-section **Paramètres généraux**.
3. Dans le groupe **Protection interactive**, décochez ou cochez les cases selon le mode de protection que vous avez sélectionné :
   - Pour installer le mode de protection interactif, décochez la case **Sélectionner l'action automatiquement** ;
   - Pour installer le mode de protection automatique, cochez la case **Sélectionner l'action automatiquement**.

     Si vous ne souhaitez pas que Kaspersky Anti-Virus supprime les objets suspects en mode automatique, cochez la case **Ne pas supprimer les objets suspects**.

ANALYSE DE L'ORDINATEUR

L'analyse de l'ordinateur sur les vulnérabilités, sur les virus et sur d'autres applications présentant une menace, est une des tâches principale pour en assurer la protection.

Il est indispensable de rechercher la présence éventuelle de virus et d'autres applications qui présentent une menace à intervalle régulier afin d'éviter la propagation de programmes malveillants qui n'auraient pas été découverts par les composants de la protection, par exemple en raison d'un niveau de protection trop faible ou pour toute autre raison.

La recherche de vulnérabilités consiste à fonder un diagnostic sur la sécurité du système d'exploitation et à identifier dans les applications les particularités qui pourraient être exploitées par des individus malintentionnés désireux de diffuser des objets malveillants ou d'accéder aux données personnelles.

Cette section contient des informations détaillées sur les particularités et les paramètres des tâches d'analyse ainsi que sur les niveaux de protection, les méthodes et les technologies d'analyse.

DANS CETTE SECTION

RECHERCHE DE VIRUS

Kaspersky Anti-Virus propose les tâches suivantes pour la recherche de virus et d'autres applications présentant une menace :

- **Analyse complète**. Analyse de tout le système. Kaspersky Anti-Virus analyse par défaut les objets suivants :
  - mémoire système ;
  - objets téléchargés au démarrage du système d'exploitation ;
  - sauvegarde ;
  - bases de messagerie ;
  - disques durs, disques de réseau et disques amovibles.

- **Analyse rapide**. Kaspersky Anti-Virus analyse par défaut les objets chargés au démarrage du système d'exploitation.
- **Analyse personnalisée**. Kaspersky Anti-Virus analyse les objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet de la liste suivante :
  - mémoire système ;
  - objets chargés au démarrage du système d'exploitation ;
  - sauvegarde ;
  - bases de messagerie ;
  - disques durs, disques de réseau et disques amovibles ;
  - n'importe quel fichier ou dossier sélectionné.

Les tâches d'analyse complète et d'analyse des secteurs importants sont des tâches spécifiques. Pour ces tâches, il est déconseillé de modifier la liste des objets à analyser.

Chaque tâche d'analyse est exécutée dans une zone définie et peut être lancée selon un horaire défini. De plus, chaque tâche d'analyse se distingue par un niveau de protection (ensemble de paramètres qui exercent une influence sur la minutie de l'analyse). Le *mode de signature* : un mode de recherche des menaces à l'aide des enregistrements présents dans les bases de l'application - est toujours activé par défaut. De plus, il est possible d'impliquer diverses méthodes et technologies d'analyse.

Après le lancement de la tâche d'analyse complète ou d'analyse rapide, la progression de celles-ci est présentée dans la fenêtre **Analyse** dans le groupe sous le nom de la tâche exécutée et dans Gestionnaire des tâches (cf. section "Administration des tâches d'analyse. Gestionnaire de tâches" à la page 73).

Dès que Kaspersky Anti-Virus identifie une menace, il attribue un des états suivants à l'objet détecté :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* (suspect) lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Le fichier contient peut-être une séquence de code propre aux virus ou la modification d'un code de virus connu.

Ensuite, l'application affiche une notification (cf. page 127) sur la menace détectée et exécute l'action définie. Vous pouvez modifier l'action exécutée après la découverte d'une menace.

Si vous travaillez en mode automatique (cf. section "Sélection du mode de protection" à la page 64), Kaspersky Anti-Virus appliquera automatiquement les actions recommandées par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, cette action sera **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**. Si vous travailler dans le mode interactif (cf. section "Sélection du mode de protection" à la page 64), lors de la détection d'objets dangereux l'application affiche une notification dans laquelle vous allez pouvoir sélectionner l'action parmi celles proposées.

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus crée une copie de sauvegarde au cas où la restauration de l'objet serait requise ou si la possibilité de le réparer se présentait. Les objets suspects (potentiellement infectés) sont placés en quarantaine. Vous pouvez activer l'analyse automatique des fichiers en quarantaine après chaque mise à jour.

Les informations relatives aux résultats de l'analyse et à tous les événements survenus pendant l'exécution des tâches sont consignées dans le .rapport de Kaspersky Anti-Virus (cf. page 122).

DANS CETTE SECTION

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION

En fonction de vos besoins actuels, vous pouvez choisir un des niveaux prédéfinis de la protection ou configurer vous-même les paramètres.

Une fois que vous aurez configuré les paramètres d'exécution de la tâche de l'analyse, sachez que vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Afin de modifier le niveau de protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée, dans le groupe **Niveau de protection**, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

> En cas de configuration manuelle, l'appellation du niveau de protection devient **Autre**.

Pour restaurer les paramètres d'analyse recommandés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Par défaut**.

PROGRAMMATION DE L'EXECUTION DE L'ANALYSE

Il est possible d'exécuter les tâches automatiquement en les programmant, à savoir en définissant la fréquence d'exécution de la tâche, l'heure d'exécution (le cas échéant), ainsi que des paramètres complémentaires.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible. De plus, il est possible de programmer l'arrêt automatique de l'analyse quand l'économiseur d'écran se désactive ou quand l'ordinateur est déverrouillé. Cette possibilité permet de reporter le lancement de la tâche jusqu'à ce que l'utilisateur termine son travail sur l'ordinateur. Ainsi, la tâche d'analyse n'occupera pas les ressources de l'ordinateur pendant son exécution.

Le mode spécial d'analyse pendant le temps mort (cf. section "Lancement des tâches en arrière-plan" à la page 111) permet de lancer l'analyse de la mémoire système, du système et des objets de démarrage lorsque l'ordinateur n'est pas utilisé.

Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Recherche de vulnérabilités**).
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Mode d'exécution**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution** dans le groupe **Programmation**, sélectionnez l'option **Selon la programmation**, puis configurer le mode d'exécution de l'analyse, en indiquant les valeurs requises du paramètre **Fréquence**.

Pour activer l'exécution automatique d'une tâche d'analyse qui n'aurait pas été exécutée, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Recherche de vulnérabilités**).
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Mode d'exécution**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation**, sélectionnez l'option **Selon la programmation**, puis cochez la case **Lancer les tâches non exécutées**.

Pour lancer l'analyse une fois que l'utilisateur aura terminé son travail, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Recherche de vulnérabilités**).
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Mode d'exécution**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution** dans le groupe **Programmation**, sélectionnez l'option **Selon la programmation** et cochez la case **Suspendre l'analyse selon la programmation si l'écran de veille est actif et l'ordinateur est débloqué**.

COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

Une liste d'objets à analyser est associée par défaut à chaque tâche de recherche d'éventuels virus. Ces objets peuvent être des objets du système de fichiers de l'ordinateur (par exemple, les disques logiques, les bases de messagerie) ainsi que des objets d'autres types (par exemple, des disques de réseau). Vous pouvez introduire des modifications dans cette liste.

Si la zone d'analyse est vide ou si aucun des objets qu'elle contient n'a été coché, il ne sera pas possible de lancer la tâche d'analyse.

Pour composer la liste des objets pour la tâche d'analyse personnalisée, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.
3. Dans la partie inférieure de la fenêtre, à l'aide du lien **désignez** ouvrez la liste des objets à analyser.
4. Dans la fenêtre **Analyse personnalisée** qui s'ouvre, cliquez sur **Ajouter**.
5. Dans la fenêtre **Sélection de l'objet à analyser** qui s'ouvre, sélectionnez l'objet et cliquez sur le bouton **Ajouter**. Une fois que vous aurez ajouté tous les objets requis, cliquez sur le bouton **OK**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

   Vous pouvez également transférer directement les fichiers à analyser dans un secteur spécial de la section **Analyse**.

Pour former la liste des objets pour la tâche d'analyse complète, d'analyse des zones importantes ou de recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche d'analyse requise (**Analyse complète**, **Analyse rapide** ou **Recherche de vulnérabilités**).
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Objets à analyser**.
4. Dans la fenêtre ouverte **Objets à analyser**, à l'aide des boutons **Ajouter**, **Modifier**, **Supprimer**, formez la liste. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

   Les objets ajoutés à la liste par défaut ne peuvent être modifiés ou supprimés.

SELECTION DES METHODES D'ANALYSE

La recherche d'éventuels virus sur l'ordinateur s'opère toujours selon l'*analyse sur la base des signatures* au cours de laquelle Kaspersky Anti-Virus compare l'objet trouvé aux bases de signatures.

Pour renforcer l'efficacité de la recherche, vous pouvez activer des méthodes d'analyse complémentaires : *analyse heuristique* (analyse de l'activité de l'objet dans le système) et *recherche d'outils de dissimulation d'activité* (utilitaires qui permettent de dissimuler les programmes malveillants dans le système d'exploitation).

Pour sélectionner les méthodes d'analyse requises, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Méthodes d'analyse**, définissez les modes d'analyse requis.

SELECTION DE LA TECHNOLOGIE D'ANALYSE

Outre le choix des méthodes d'analyse, vous pouvez faire intervenir des technologies d'analyse des objets spéciales qui permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

Pour sélectionner les technologies d'analyse des objets, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Technologies d'analyse**, définissez les paramètres requis.

MODIFICATION DE L'ACTION A EXECUTER APRES LA DECOUVERTE D'UNE MENACE

En cas de découverte d'objets infectés, l'application exécute l'action définie.

Pour modifier l'action à exécuter suite à la découverte d'une menace, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Dans la partie droite de la fenêtre, dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'option requise.

LANCEMENT DE L'ANALYSE SOUS LES PRIVILEGES D'UN AUTRE UTILISATEUR

La tâche d'analyse est lancée par défaut sous le compte que vous avez utilisé pour ouvrir votre session dans le système. Toutefois, il peut s'avérer parfois nécessaire d'exécuter une tâche sous les privilèges d'un autre utilisateur. Vous pouvez désigner le compte utilisateur sous les privilèges duquel chaque tâche d'analyse sera exécutée.

Pour lancer l'analyse sous les privilèges d'un autre utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Recherche de vulnérabilités**).
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Mode d'exécution**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur** cochez la case **Lancer la tâche avec les privilèges de l'utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

MODIFICATION DU TYPE D'OBJETS A ANALYSER

La définition du type d'objet à analyser est la fonction qui vous permet d'indiquer le format des fichiers qui seront analysés lors de l'exécution de la tâche d'analyse sélectionnée.

Lors de la sélection du type de fichiers, rappelez-vous des éléments suivants :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple TXT) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, EXE, DLL, DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.

- Un individu malintentionné peut envoyer un virus sur votre ordinateur dans un fichier exécutable renommé en fichier txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format EXE. Le fichier sera alors soumis à une analyse antivirus minutieuse.

Afin de modifier les types de fichiers à analyser, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Types de fichiers**, sélectionnez le paramètre requis.

ANALYSE DES FICHIERS COMPOSES

La dissimulation de virus dans des fichiers composés tels que des archives, des paquets d'installation, des objets OLE joints ou des fichiers au format de messagerie est très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour réaliser la sélection, cliquez sur le lien situé à côté du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si le mode d'analyse uniquement des nouveaux fichiers ou des fichiers modifiés (cf. page 72) est sélectionné, les liens pour la sélection de l'analyse de tous les fichiers ou des nouveaux fichiers uniquement seront inaccessibles.

Vous pouvez également définir la taille maximale du fichier composé à analyser. Les fichiers composés dont la taille dépasse la valeur définie ne seront pas analysés.

Lors de l'extraction d'archives, les fichiers de grande taille seront soumis à l'analyse antivirus même si la case **Ne pas décompacter les fichiers composés de grande taille** est cochée.

Pour modifier la liste des fichiers composés à analyser, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Analyse des fichiers composés**, sélectionnez les types de fichiers composés à analyser.

Pour définir la taille maximale des fichiers composés qui seront analysés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Zone d'action**.
5. Dans la fenêtre **Fichiers composés** qui s'ouvre, cochez la case **Ne pas décompacter les fichiers composés de grande taille** et définissez la taille maximale des fichiers à analyser.

OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Anti-Virus. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

Il est également possible de limiter la durée de l'analyse d'un objet. A l'issue du temps défini, l'objet sera exclu de l'analyse en cours (sauf les archives et les fichiers incluant quelques objets).

Afin d'analyser uniquement les nouveaux fichiers et les fichiers modifiés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

Pour limiter la durée de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la section **Analyse de l'ordinateur** la tâche requise (**Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Optimisation de l'analyse**, cochez la case **Ignorer les objets si l'analyse dure plus de** et définissez la durée d'analyse d'un fichier.

ANALYSE DES DISQUES AMOVIBLES A LA CONNEXION

Ces derniers temps, les objets malveillants qui exploitent les vulnérabilités du système d'exploitation pour se diffuser via les réseaux locaux et les disques amovibles sont fort répandus. Kaspersky Anti-Virus prend en charge la recherche de virus sur les disques amovibles lorsque ceux-ci sont connectés à l'ordinateur.

Pour configurer l'analyse des disques amovibles lors de leur connexion à l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Analyse de l'ordinateur**, sélectionnez la section **Paramètres généraux**.

3. Dans le groupe **Analyse des disques amovibles à la connexion**, sélectionnez l'action et, le cas échéant, définissez la taille maximale du disque à analyser dans le champ inférieur.

CREATION D'UN RACCOURCI POUR LE LANCEMENT D'UNE TACHE

L'application prend en charge la création de raccourcis pour accélérer le lancement des analyses complètes et rapides ou de la recherche de vulnérabilités. Il est ainsi possible de lancer la tâche d'analyse requise sans devoir ouvrir la fenêtre principale de l'application ou le menu contextuel.

Pour créer un raccourci pour le lancement de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Analyse de l'ordinateur**, sélectionnez la section **Paramètres généraux**.
3. Dans la partie droite de la fenêtre, dans le groupe **Lancement rapide des tâches**, cliquez sur le lien **Créer un raccourci** situé à côté du nom de la tâche envisagée (**Analyse rapide** ou **Analyse complète** ou **Recherche de Vulnérabilités**).
4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du raccourci ainsi que son nom. Par défaut, le raccourci prend le nom de la tâche et est créé dans le répertoire Poste de travail de l'utilisateur actuel de l'ordinateur.

RECHERCHE DE VULNERABILITES

Des vulnérabilités peuvent exister dans un système d'exploitation, par exemple en raison d'une erreur de programmation, à cause de mots de passe faibles ou d'actions de programmes malveillants. Dans la cadre de la recherche de vulnérabilités, l'application adopte diverses mesures de sécurité, par exemple l'étude du système, l'analyse des paramètres du système d'exploitation, du navigateur ainsi que la recherche des services vulnérables.

Le diagnostic peut durer un certain temps. Une fois qu'un problème a été identifié, il est analysé pour déterminer le danger qu'il représente.

Une fois la tâche de recherche des vulnérabilités exécutée (cf. page 48), vous pouvez suivre sa progression dans la fenêtre **Analyse** dans le groupe **Recherche de Vulnérabilités**, ainsi que dans le Gestionnaire de tâches (cf. section "Administration des tâches d'analyse. Gestionnaire de tâches" à la page 73).

Les informations sur les résultats d'exécution des tâches de recherche de vulnérabilités sont enregistrées dans le rapport de Kaspersky Anti-Virus (cf. page 122).

Tout comme pour les tâches de recherche de virus, il est possible de programmer l'exécution de recherche de vulnérabilités, de composer la liste des objets à analyser (cf. page 68), de sélectionner le compte utilisateur (cf. section "Lancement de l'analyse sous les privilèges d'un autre utilisateur" à la page 70) et de créer un raccourci pour l'exécution rapide de la tâche. Par défaut, les applications installées sont choisies en guise d'objets à analyser.

ADMINISTRATION DES TACHES D'ANALYSE. GESTIONNAIRE DE TACHES

Le Gestionnaire de tâches affiche les informations relatives aux dernières tâches exécutées ou aux tâches en cours d'exécution (par exemple, recherche de virus, recherche de vulnérabilités, recherche d'outils de dissimulation d'activité, réparation de l'infection active).

Le Gestionnaire de tâches permet de consulter le processus et le résultat de l'exécution de la tâche ou d'arrêter la tâche. Des actions complémentaires sont disponibles pour certaines tâches (par exemple, à l'issue de la recherche de vulnérabilités, vous pouvez ouvrir la liste des vulnérabilités détectées et y remédier).

Pour ouvrir le Gestionnaire de tâches, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.
3. Dans la fenêtre **Analyse** qui s'ouvre, cliquez sur le bouton **Gestionnaire de tâches** dans le coin supérieur droit de la fenêtre.

MISE A JOUR

La mise à jour des bases et des modules logiciels de Kaspersky Anti-Virus préserve l'actualité de la protection de votre ordinateur. Chaque jour, de nouveaux virus, chevaux de Troie et autres programmes malveillants apparaissent dans le monde. Les bases de Kaspersky Anti-Virus contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour détecter de nouvelles menaces en permanence, il vous faut donc régulièrement actualiser les bases et les modules logiciels.

La mise à jour régulière requiert une licence d'utilisation de l'application valide. En l'absence d'une telle licence, vous ne pourrez réaliser la mise à jour qu'une seule fois.

Lors de la mise à jour de l'application, les objets suivants sont téléchargés et installés sur votre ordinateur :

- Bases de Kaspersky Anti-Virus.

  La protection des données est garantie par l'utilisation de bases de données qui contiennent les signatures des menaces, les descriptions des attaques de réseau ainsi que les méthodes de lutte contre celles-ci. Elles sont utilisées par les composants de la protection pour rechercher les objets dangereux sur votre ordinateur et les neutraliser. Ces bases sont enrichies régulièrement avec les définitions des nouvelles menaces et les moyens de lutter contre celles-ci. Pour cette raison, il est vivement recommandé d'actualiser régulièrement les bases.

  En plus des bases de Kaspersky Anti-Virus, la mise à jour concerne également les pilotes de réseau qui assurent l'interception du trafic de réseau par les composants de la protection.

- Modules logiciels.

  Outre les bases de Kaspersky Anti-Virus, il est possible d'actualiser les modules logiciels. Les mises à jour des modules logiciels permettent de supprimer les vulnérabilités de Kaspersky Anti-Virus, ajoutent de nouvelles fonctionnalités ou améliorent celles existantes.

Au cours du processus de mise à jour, les modules logiciels et les bases installés sur votre ordinateur sont comparés à ceux présents sur la source des mises à jour. Si les bases et les modules logiciels actuels diffèrent de la version à jour, la partie manquante sera installée sur l'ordinateur.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Avant d'actualiser les bases, Kaspersky Anti-Virus crée une copie de sauvegarde au cas où vous souhaiteriez les utiliser à nouveau dans une version antérieure (cf. section "Annulation de la dernière mise à jour" à la page 78).

Les informations relatives à l'état actuel des bases de Kaspersky Anti-Virus sont affichées dans la section **Mise à jour** de la fenêtre principale de l'application.

Les informations relatives aux résultats de la mise à jour et à tous les événements survenus pendant l'exécution des tâches sont consignées dans le rapport de Kaspersky Anti-Virus (cf. page 122).

Vous pouvez sélectionner la source des mises à jour (cf. section "Sélection de la source de mises à jour" à la page 75) ainsi que configurer les paramètres de lancement automatique de celle-ci.

DANS CETTE SECTION

SELECTION DE LA SOURCE DE MISES A JOUR

La source des mises à jour est une ressource qui contient les mises à jour des bases et des modules logiciels de Kaspersky Anti-Virus.

Les serveurs de mise à jour de Kaspersky Lab, qui hébergent les mises à jour des bases et des modules pour tous les produits de Kaspersky Lab, sont la principale source de mises à jour.

Pour que le téléchargement des mises à jour depuis les serveurs réussisse, l'ordinateur doit être connecté à Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si vous utilisez un serveur proxy, il faudra peut-être configurer les paramètres de connexion (cf. section "Configuration des paramètres du serveur proxy" à la page 106).

Pendant la mise à jour de Kaspersky Anti-Virus, vous pouvez copier les mises à jour des bases et des modules récupérés sur les serveurs de Kaspersky Lab dans un dossier local (cf. section "Mise à jour depuis un dossier partagé" à la page 76), puis octroyer l'accès à ce répertoire aux autres ordinateurs du réseau. Vous économiserez ainsi du trafic Internet.

Lors de la commande des mises à jour sur disque amovible, précisez si vous souhaitez recevoir la mise à jour des modules logiciels.

AJOUT D'UNE SOURCE DE MISES A JOUR

Par défaut, la liste des sources de mises à jour contient uniquement les serveurs de mise à jour de Kaspersky Lab. Vous pouvez ajouter un dossier local ou un autre serveur en guise de source de mises à jour. Si plusieurs ressources ont été sélectionnées en guise de sources de mise à jour, Kaspersky Anti-Virus les consultera dans l'ordre de la liste et réalisera la mise à jour au départ de la première source disponible.

➧ *Pour ajouter une source de mises à jour, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Source des mises à jour**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Source**, ouvrez la fenêtre de sélection en cliquant sur le bouton **Ajouter**.
5. Dans la fenêtre **Source des mises à jour** qui s'ouvre, sélectionnez le dossier contenant les mises à jour ou saisissez l'adresse du serveur sur lequel il faut récupérer les mises à jour dans le champ **Source**.

SELECTION DE LA REGION DU SERVEUR DE MISES A JOUR

Si vous utilisez les serveurs de Kaspersky Lab en guise de source de mises à jour, vous pouvez sélectionner le serveur en fonction de la situation géographique qui vous convient le mieux. Les serveurs de Kaspersky Lab sont répartis dans plusieurs pays.

En utilisant le serveur de mise à jour de Kaspersky Lab le plus proche, vous réduirez la durée nécessaire à la récupération des mises à jour. Par défaut, la sélection s'opère sur la base des informations géographiques reprises dans la base de registres système. Vous pouvez choisir la région manuellement.

Pour choisir la région du serveur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Source des mises à jour**.
4. Dans la fenêtre qui s'ouvre sous l'onglet **Source**, dans le groupe **Serveur proxy**, sélectionnez l'option **Choisir dans la liste** et, dans la liste déroulante, sélectionnez le pays le plus proche de votre situation géographique actuelle.

MISE A JOUR DEPUIS UN DOSSIER PARTAGE

Afin d'économiser le trafic Internet, il est possible de configurer la mise à jour de Kaspersky Anti-Virus sur les ordinateurs du réseau depuis le dossier partagé. Dans ce cas, un des ordinateurs du réseau récupère les mises à jour depuis les serveurs de Kaspersky Lab ou depuis une autre ressource en ligne contenant la version la plus récente des mises à jour. Les mises à jour récupérées sont copiées dans un dossier partagé. Les autres ordinateurs de réseau accèdent à ce dossier pour récupérer les mises à jour de Kaspersky Anti-Virus.

Lors du travail sous le compte visiteur sous Microsoft Windows 7, les mises à jour ne sont pas copiées dans le dossier partagé. Il est recommandé de se connecter sous un autre compte pour pouvoir copier les mises à jour.

Pour activer le mode de copie des mises à jour, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Avancé**, cochez la case **Copier la mise à jour des bases dans le dossier** et dans le champ en dessous, saisissez le chemin d'accès au dossier partagé où seront stockées les mises à jour récupérées. Vous pouvez également choisir le dossier en cliquant sur le bouton **Parcourir**.

Pour télécharger les mises à jour pour l'ordinateur depuis le dossier partagé indiqué, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Source des mises à jour**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Source**, ouvrez la fenêtre de sélection en cliquant sur le bouton **Ajouter**.

5. Dans la fenêtre **Source des mises à jour** qui s'ouvre, sélectionnez le répertoire ou saisissez son chemin d'accès complet dans le champ **Source**.

6. Sous l'onglet **Source**, désélectionnez la case **Serveurs de mise à jour de Kaspersky Lab**.

PROGRAMMATION DE L'EXECUTION DE LA MISE A JOUR

Il est possible d'exécuter les tâches de mise à jour automatiquement en les programmant, à savoir en définissant la fréquence d'exécution de la tâche, l'heure d'exécution (le cas échéant), ainsi que des paramètres complémentaires.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible.

Vous pouvez également reporter le lancement automatique des tâches après le démarrage de l'application. Dans ce cas, toutes les tâches programmées seront lancées uniquement une fois que le délai défini après le démarrage de Kaspersky Anti-Virus sera écoulé.

Ce mode particulier d'analyse pendant les temps morts de l'ordinateur (cf. section "Lancement des tâches en arrière-plan" à la page 111) est prévu pour optimiser la charge des ressources de l'ordinateur.

- *Pour programmer l'exécution de la tâche de mise à jour, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.

  2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.

  3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Mode d'exécution**.

  4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution** dans le groupe **Programmation**, sélectionnez l'option **Selon la programmation**, puis configurez le mode d'exécution de la mise à jour.

- *Pour activer l'exécution automatique d'une tâche d'analyse qui n'aurait pas été exécutée, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.

  2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.

  3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Mode d'exécution**.

  4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation**, sélectionnez l'option **Selon la programmation**, puis cochez la case **Lancer les tâches non exécutées**.

- *Pour reporter l'exécution des tâches après le démarrage de l'application, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.

  2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.

  3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Mode d'exécution**.

  4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution** dans le groupe **Programmation**, sélectionnez l'option **Selon la programmation**, puis indiquez la durée du report dans le champ **Intervalle entre le lancement et le démarrage de l'application**.

ANNULATION DE LA DERNIERE MISE A JOUR

Après la première mise à jour de Kaspersky Anti-Virus, vous aurez la possibilité de revenir à l'état antérieur à la mise à jour.

La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Anti-Virus bloque une application sans danger.

Si les bases sont endommagées, Kaspersky Anti-Virus recommande de lancer la tâche de mise à jour afin de télécharger de nouveau sur les bases actuelles.

Pour revenir à l'utilisation de la version précédente des bases, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Mise à jour**.
3. Dans la fenêtre ouverte **Mise à jour**, cliquez sur le bouton et dans le menu ouvert sélectionnez l'option **Restaurer les mises à jour précédentes**.

LANCEMENT DE LA MISE A JOUR AVEC LES PRIVILEGES D'UN AUTRE UTILISATEUR

La mise à jour est lancée par défaut sous le compte que vous avez utilisé pour ouvrir votre session dans le système. Il arrive parfois que la mise à jour de Kaspersky Anti-Virus se déroule depuis une source à laquelle vous n'avez pas accès (par exemple, le répertoire de réseau contenant des mises à jour) ou pour laquelle vous ne bénéficiez pas des privilèges d'utilisateur autorisé du serveur proxy. Vous pouvez lancer la mise à jour de Kaspersky Anti-Virus au nom d'un utilisateur possédant ces privilèges.

Pour lancer la mise à jour sous les privilèges d'un autre utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Mode d'exécution**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur** cochez la case **Lancer la tâche avec les privilèges de l'utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

UTILISATION DU SERVEUR PROXY

Si l'accès à Internet s'opère via un serveur proxy, il faut configurer ses paramètres afin de réussir la mise à jour de Kaspersky Anti-Virus.

Pour configurer les paramètres du serveur proxy, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Source des mises à jour**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Source**, cliquez sur le lien **Serveur proxy**.

5. Dans la fenêtre **Paramètres du serveur proxy** qui s'ouvre, configurez les paramètres du serveur proxy.

ANTIVIRUS FICHIERS

L'Antivirus Fichiers permet d'éviter l'infection du système de fichiers de l'ordinateur. Le composant est lancé au démarrage du système d'exploitation. Il se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les fichiers ouverts, enregistrés et exécutés sur l'ordinateur ainsi que sur tous les disques montés. Il recherche des virus et d'autres applications présentant une menace.

Vous pouvez désigner une zone de protection et sélectionner le niveau de la protection (ensemble de paramètres ayant une influence sur la minutie de l'analyse).

Lorsque l'utilisateur ou une application sollicite le fichier protégé, l'Antivirus Fichiers recherche les données relatives à celui-ci dans les bases iChecker et iSwift et, sur la base des données obtenues, décide d'analyser ou non le fichier.

L'*analyse de signature* - un mode de recherche des menaces à l'aide des enregistrements dans les bases de l'application - est toujours activée par défaut. De plus, il est possible d'utiliser également l'analyse heuristique et diverses technologies d'analyse.

Lors de la détection d'une menace dans le fichier, Kaspersky Anti-Virus attribue au fichier un des états suivants :

- Etat qui désigne le type de l'application malveillante détectée (par exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* (suspect) lorsqu'il est impossible d'affirmer avec certitude si le fichier est infecté ou non. Le fichier contient peut-être une séquence de code propre aux virus et aux autres applications présentant une menace ou la modification d'un code de virus connu.

Ensuite, l'application affiche une notification (cf. page 127) sur la menace détectée et exécute l'action définie sur le fichier dans les paramètres de l'Antivirus Fichiers. Vous pouvez modifier l'action (cf. page 84) que l'application doit exécuter lors de la détection d'une menace.

Si vous travaillez en mode automatique (cf. section "Sélection du mode de protection" à la page 64), Kaspersky Anti-Virus appliquera automatiquement les actions recommandées par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, cette action sera **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**. Si vous travailler dans le mode interactif (cf. section "Sélection du mode de protection" à la page 64), lors de la détection d'objets dangereux l'application affiche une notification dans laquelle vous allez pouvoir sélectionner l'action parmi celles proposées.

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus crée une copie de sauvegarde au cas où la restauration de l'objet serait requise ou si la possibilité de le réparer se présentait. Les objets suspects (potentiellement infectés) sont placés en quarantaine. Vous pouvez activer l'analyse automatique des fichiers en quarantaine après chaque mise à jour.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS FICHIERS

Par défaut, l'Antivirus Fichiers est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Fichiers le cas échéant.

Pour désactiver l'utilisation de l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus Fichiers**.

ARRET AUTOMATIQUE DE L'ANTIVIRUS FICHIERS

Lors de l'exécution de tâches qui requièrent des ressources importantes du système d'exploitation, il est possible de suspendre le fonctionnement de l'Antivirus Fichiers. Pour réduire la charge et garantir un accès rapide aux objets, vous pouvez configurer l'arrêt automatique du composant à l'heure indiquée ou en cas d'utilisation d'une application en particulier.

La suspension de l'Antivirus Fichiers en cas de conflit avec certaines applications est une mesure extrême. Si des conflits se manifestent pendant l'utilisation du composant, veuillez contacter le Support technique de Kaspersky Lab (http://support.kaspersky.com/fr). Les experts vous aideront à garantir le fonctionnement de Kaspersky Anti-Virus avec d'autres applications sur votre ordinateur.

Pour suspendre le fonctionnement du composant à une heure définie, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case **Selon la programmation**, puis cliquez sur **Programmation**.
5. Dans la fenêtre **Suspension de la tâche**, indiquez la durée (au format hh:mm) pendant laquelle la protection sera suspendue (champs **Pause à partir de** et **Reprendre à**).

Pour suspendre le fonctionnement du composant lors du lancement de certaines applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case **Au lancement du programme** puis cliquez sur Sélection.

5. Dans la fenêtre **Applications**, composez la liste des applications pendant l'utilisation desquelles le composant sera suspendu.

FORMATION DE LA ZONE DE PROTECTION DE L'ANTIVIRUS FICHIERS

La zone de protection fait référence à l'emplacement et au type d'objets analysés. Kaspersky Anti-Virus analyse par défaut uniquement les fichiers qui pourraient être infectés et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques de réseau.

Pour former la zone de protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre ouverte sous l'onglet **Général** dans le groupe **Types de fichiers**, indiquez le type de fichiers que vous voulez analyser par l'Antivirus Fichiers:

   - Si vous voulez analyser tous les fichiers, sélectionnez **Tous les fichiers**.

   - Si vous voulez analyser les fichiers dont les formats sont plus exposés à l'infection, sélectionnez **Fichiers analysés selon le format**.

   - Si vous voulez analyser les fichiers avec les extensions les plus exposées à l'infection; sélectionnez **Fichiers analysés selon l'extension**.

   Lors de la sélection du type de fichiers à analyser, rappelez-vous des éléments suivants :

   - La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple TXT) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, EXE, DLL, DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.

   - Le malfaiteur peut envoyer un virus ou une autre application présentant une menace sur votre ordinateur dans le fichier exécutable en tant que fichier avec un autre nom avec l'extension txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format EXE. Un tel fichier est scrupuleusement analysé sur les virus et sur d'autres applications présentant une menace.

5. La liste **Zone d'analyse** permet d'effectuer une des actions suivantes :

   - Si vous voulez ajouter un nouvel objet à la liste des objets analysés, passez au lien **Ajouter**.

   - Si vous voulez modifier l'emplacement de l'objet, sélectionnez l'objet dans la liste et passez au lien **Modifier**.

   La fenêtre **Sélection de l'objet à analyser** s'ouvre.

   - Si vous voulez supprimer l'objet de la liste des objets à analyser, sélectionnez l'objet dans la liste et passez au lien **Supprimer**.

     La fenêtre de confirmation de suppression s'ouvrira.

6. Exécutez une des actions suivantes :

   - Si vous voulez ajouter un nouvel objet à la liste des objets analysés, dans la fenêtre **Sélection de l'objet à analyser**, sélectionnez l'objet et cliquez sur le bouton **OK**.

   - Si vous voulez modifier l'emplacement de l'objet, dans la fenêtre **Sélection de l'objet à analyser**, modifiez le chemin d'accès à l'objet dans le champ **Objet** et cliquez sur le bouton **OK**.

   - Si vous voulez supprimer l'objet de la liste des objets analyser, dans la fenêtre de confirmation de suppression, cliquez sur le bouton **Oui**.

7. Le cas échéant, répétez les points 6 et 7 pour ajouter, modifier l'emplacement ou supprimer les objets de la liste des objets analysés.

8. Pour exclure l'objet de la liste des objets analysés, décochez la case en regard de l'objet dans la liste **Zone d'analyse**. Avec cela, l'objet reste dans la liste des objets analysés mais sera exclu de l'analyse par l'Antivirus Fichiers.

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION DES FICHIERS

En fonction des besoins actuels, vous pourrez choisir un des niveaux de protection prédéfinis pour les fichiers et la mémoire ou configurer vous-même les paramètres de fonctionnement de l'Antivirus Fichiers.

Sachez que si vous configurez les paramètres de fonctionnement de l'Antivirus Fichiers, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Afin de modifier le niveau de protection des fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.

3. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

   En cas de configuration manuelle, l'appellation du niveau de protection devient **Autre**.

Pour restaurer le niveau de protection des fichiers par défaut, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.

3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

SELECTION DU MODE D'ANALYSE DES FICHIERS

Le *mode d'analyse* désigne la condition dans laquelle l'Antivirus Fichier va commencer l'analyse des fichiers. Kaspersky Anti-Virus utilise par défaut le mode intelligent. Dans ce mode d'analyse des fichiers, l'Antivirus Fichiers prend une décision sur la base de l'analyse des opérations exécutées par l'utilisateur sur les fichiers et sur la base du type de fichiers. Par exemple, dans le cas d'un fichier Microsoft Office, Kaspersky Anti-Virus analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires sur le fichier sont exclues de l'analyse.

Afin de modifier le mode d'analyse des fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Mode d'analyse**, sélectionnez le mode requis.

Lorsque vous choisissez le mode d'analyse, il faut tenir compte du type de fichiers que vous manipulez le plus souvent.

UTILISATION DE L'ANALYSE HEURISTIQUE LORS DU FONCTIONNEMENT DE L'ANTIVIRUS FICHIERS

L'Antivirus Fichiers utilise toujours l'*analyse sur la base des signatures* au cours de laquelle Kaspersky Anti-Virus compare l'objet trouvé aux bases de signatures.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

Pour activer l'utilisation de l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans le groupe **Méthode d'analyse**, cochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse.

SELECTION DE LA TECHNOLOGIE D'ANALYSE DES FICHIERS

En plus de l'analyse heuristique, vous pouvez faire intervenir des technologies particulières qui permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

Pour sélectionner les technologies d'analyse des objets, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Technologies d'analyse**, définissez les paramètres requis.

MODIFICATION DE L'ACTION SUR LES FICHIERS INFECTES

En cas de découverte d'objets infectés, l'application exécute l'action définie.

Pour modifier l'action à exécuter sur les fichiers infectés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'option requise.

ANALYSE DE FICHIERS COMPOSES PAR L'ANTIVIRUS FICHIERS

La dissimulation de virus dans des fichiers composés tels que des archives, des paquets d'installation, des objets OLE joints ou des fichiers au format de messagerie est très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour réaliser la sélection, cliquez sur le lien situé à côté du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si uniquement le mode d'analyse des nouveaux fichiers ou des fichiers modifiés est sélectionné, les liens pour la sélection de l'analyse de tous les fichiers ou uniquement des nouveaux fichiers seront inaccessibles.

Kaspersky Anti-Virus analyse par défaut uniquement les objets OLE joints.

Lors de l'analyse de fichiers composés de grande taille, le décompactage préalable peut prendre un certain temps. Il est possible de réduire la durée en activant le décompactage en arrière-plan des fichiers composés dont la taille dépasse la limite définie. Si un objet malveillant est découvert pendant l'utilisation de ces fichiers, Kaspersky Anti-Virus vous le signale.

Vous pouvez également définir la taille maximale du fichier composé à analyser. Les fichiers composés dont la taille dépasse la valeur définie ne seront pas analysés.

Lors de l'extraction d'archives, les fichiers de grande taille seront soumis à l'analyse antivirus même si la case **Ne pas décompacter les fichiers composés de grande taille** est cochée.

Pour modifier la liste des fichiers composés à analyser, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**, sélectionnez les types de fichiers composés à analyser.

Pour définir la taille maximale des fichiers composés qui seront analysés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

4. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**.

5. Dans la fenêtre **Fichiers composés**, cochez la case **Ne pas décompacter les fichiers composés de grande taille** et définissez la taille maximale des fichiers à analyser.

Pour décompacter les fichiers composés de grande taille en arrière plan, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.

3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.

4. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Performance**.

5. Dans la fenêtre **Fichiers composés**, cochez la case **Décompacter les fichiers composés en arrière-plan** et définissez la taille minimale du fichier dans le champ en dessous.

OPTIMISATION DE L'ANALYSE DES FICHIERS

Vous pouvez réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Anti-Virus. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

Afin d'analyser uniquement les nouveaux fichiers et les fichiers modifiés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Fichiers**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance**, dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

ANTIVIRUS COURRIER

L'Antivirus Courrier analyse le courrier entrant et sortant à la recherche d'objets dangereux. Il est lancé au démarrage du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI1 et NNTP ainsi que les messages envoyés via des connexions sécurisées (SSL) via les protocoles POP3 et IMAP (cf. section "Analyse des connexions sécurisées" à la page 104).

L'icône de Kaspersky Internet Security dans la zone de notification de la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence  chaque fois qu'un message est analysé.

L'Antivirus Courrier intercepte et analyse chaque message reçu ou envoyé par l'utilisateur. Si aucune menace n'a été découverte, le message devient accessible à l'utilisateur.

Vous pouvez désigner les types de messages qu'il faut analyser et sélectionner le niveau de protection (cf. page 88) (ensemble de paramètres exerçant une influence sur la minutie de l'analyse).

L'*analyse de signature* - un mode de recherche des menaces à l'aide des enregistrements dans les bases de l'application - est toujours activée par défaut. Il est également possible d'utiliser l'analyse heuristique. De plus, vous pouvez activer le filtrage des pièces jointes (cf. page 89) qui permet de renommer automatiquement ou de supprimer les fichiers du type défini.

Lors de la détection d'une menace dans le fichier, Kaspersky Anti-Virus attribue au fichier un des états suivants :

- Etat qui désigne le type de l'application malveillante détectée (par exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* (suspect) lorsqu'il est impossible d'affirmer avec certitude si le fichier est infecté ou non. Le fichier contient peut-être une séquence de code propre aux virus et aux autres applications présentant une menace ou la modification d'un code de virus connu.

Ensuite, l'application bloque le message et affiche une notification (cf. page 127) sur la menace détectée et exécute l'action définie dans les paramètres de l'Antivirus Courrier. Vous pouvez modifier l'action exécutée après la découverte d'une menace (cf. section "Modification de l'action sur les messages infectés" à la page 89).

Si vous travaillez en mode automatique (cf. section "Sélection du mode de protection" à la page 64), Kaspersky Anti-Virus appliquera automatiquement les actions recommandées par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants, cette action sera **Réparer. Supprimer, si la réparation est impossible**, pour les objets suspects : **Mettre en quarantaine**. Si vous travailler dans le mode interactif (cf. section "Sélection du mode de protection" à la page 64), lors de la détection d'objets dangereux l'application affiche une notification dans laquelle vous allez pouvoir sélectionner l'action parmi celles proposées.

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus crée une copie de sauvegarde au cas où la restauration de l'objet serait requise ou si la possibilité de le réparer se présentait. Les objets suspects (potentiellement infectés) sont placés en quarantaine. Vous pouvez activer l'analyse automatique des fichiers en quarantaine après chaque mise à jour.

Si la réparation réussit, l'utilisateur peut accéder au message. Dans le cas contraire, l'objet infecté est supprimé du message électronique. L'Antivirus Courrier place au sujet du message le texte notifiant que le message a été traité par Kaspersky Anti-Virus.

Un plug-in spécial qui permet de réaliser une configuration plus fine de l'analyse du courrier a été ajouté au client de messagerie Microsoft Office Outlook.

Si vous utilisez The Bat!, Kaspersky Anti-Virus peut être utilisé conjointement à d'autres logiciels antivirus. Dans ce cas, les règles de traitement du courrier sont définies directement dans The Bat! et prévalent sur les paramètres de protection du courrier de Kaspersky Anti-Virus.

S'agissant des autres clients de messagerie populaires (dont Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail), l'Antivirus Courrier analyse le courrier entrant et sortant via les protocoles SMTP, POP3, IMAP et NNTP.

N'oubliez pas qu'en cas d'utilisation du client de messagerie Thunderbird, les messages transmis via le protocole IMAP ne sont pas soumis à l'analyse antivirus en cas d'utilisation de filtres triant les messages du dossier **Boîte aux lettres**.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS COURRIER

Par défaut, l'Antivirus Courrier est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Courrier le cas échéant.

Pour désactiver l'utilisation de l'Antivirus Courrier, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cochez la case **Activer l'Antivirus Courrier**.

FORMATION DE LA ZONE DE PROTECTION DE L'ANTIVIRUS COURRIER

La zone de protection désigne le type de messages analysés, les protocoles dont le trafic est analysé par Kaspersky Anti-Virus, ainsi que les paramètres d'intégration de l'Antivirus Courrier dans le système.

Kaspersky Anti-Virus analyse par défaut les messages entrants et sortants, s'intègre dans les clients de messagerie Microsoft Office Outlook et The Bat! et analyse le trafic des protocoles de messagerie POP3, SMTP, NNTP et IMAP.

Pour désactiver la protection du courrier sortant, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, dans le groupe **Zone de protection** de l'onglet **Général**, sélectionnez l'option **Analyser uniquement le courrier entrant**.

> Si vous avez choisi l'analyse des messages entrants uniquement, il est conseillé au tout début de l'utilisation de Kaspersky Anti-Virus d'analyser le courrier sortant car le risque existe que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. L'analyse du courrier sortant permet d'éviter les inconvénients liés à la diffusion non contrôlée des messages infectés depuis votre ordinateur.

Pour sélectionner les paramètres d'intégration de l'Antivirus Courrier au système ainsi que les protocoles à analyser, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. De groupe **Intégration au système** de l'onglet **Avancé** de la fenêtre qui s'ouvre, sélectionnez les paramètres requis.

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION DU COURRIER

En fonction des vos besoins, vous pourrez choisir un des niveaux de protection prédéfinis pour la protection du courrier ou configurer vous-même les paramètres de fonctionnement de l'Antivirus Courrier.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Courrier. Dans la majorité des cas, il suffit de sélectionner un autre niveau de protection.

Sachez que si vous configurez les paramètres de fonctionnement de l'Antivirus Courrier, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Afin de modifier le niveau de protection du courrier, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

   En cas de configuration manuelle, l'appellation du niveau de protection devient **Autre**.

Pour restaurer les paramètres de protection du courrier par défaut, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

UTILISATION DE L'ANALYSE HEURISTIQUE LORS DU FONCTIONNEMENT DE L'ANTIVIRUS COURRIER

L'Antivirus Courrier utilise toujours l'*analyse sur la base des signatures* au cours de laquelle Kaspersky Anti-Virus compare l'objet trouvé aux bases de signatures.

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

Pour activer l'utilisation de l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Méthode d'analyse** cochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse.

MODIFICATION DE L'ACTION SUR LES MESSAGES INFECTES

En cas de découverte d'objets infectés, l'application exécute l'action définie.

Pour modifier l'action à exécuter sur les messages infectés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'option requise.

FILTRAGE DES PIECES JOINTES DANS LES MESSAGES

Les applications malveillantes peuvent se diffuser via le courrier électronique sous forme de pièces jointes dans les messages. Vous pouvez configurer le filtrage selon le type des pièces jointes présentes dans les messages permettant ainsi de renommer automatiquement ou de supprimer les fichiers des types indiqués.

Pour configurer le filtrage des pièces jointes, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Filtre des pièces jointes**, sélectionnez le mode de filtrage des pièces jointes. Lorsque les deux derniers modes sont sélectionnés, la liste des types d'objet (extension) devient active. Elle vous permet de sélectionner les types requis ou d'ajouter un masque d'un nouveau type.

   Pour ajouter un masque d'un nouveau type à la liste, cliquez sur le lien **Ajouter** et ouvrez la fenêtre **Masque de nom de fichiers**, puis saisissez les données requises.

ANALYSE DE FICHIERS COMPOSES PAR L'ANTIVIRUS COURRIER

La dissimulation de virus dans des fichiers composés tels que des archives, des paquets d'installation, des objets OLE joints ou des fichiers au format de messagerie est très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Vous pouvez activer ou désactiver l'analyse des fichiers composés ainsi que limiter la taille maximum des fichiers composés à analyser.

Si votre ordinateur n'est protégé par aucun moyen du réseau local (l'accès à Internet s'opère sans serveur proxy ou pare-feu), il est déconseillé de désactiver l'analyse des fichiers composés.

Pour configurer l'analyse des fichiers composés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus Courrier**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, définissez les paramètres requis.

ANALYSE DU COURRIER DANS MICROSOFT OFFICE OUTLOOK

Lors de l'installation de Kaspersky Anti-Virus, un plug-in spécial est intégré à l'application Microsoft Office Outlook. Il permet de passer rapidement à la configuration des paramètres de l'Antivirus Courrier depuis l'application Microsoft Office Outlook et de définir comment (à la réception, à l'ouverture ou à l'envoi) analyser les messages sur la présence de virus et d'autres applications présentant une menace.

La configuration des paramètres de l'Antivirus Courrier depuis l'application Microsoft Office Outlook est accessible si cela est indiqué dans les paramètres de la zone d'analyse de l'Antivirus Courrier.

➧ *Pour configurer les paramètres de l'analyse du courrier dans l'application Microsoft Office Outlook, procédez comme suit :*

1. Ouvrez la fenêtre principale de Microsoft Office Outlook.
2. Dans le menu de l'application, sélectionnez l'option **Service** → **Paramètres**.
3. Dans la fenêtre ouverte **Paramètres**, sélectionnez l'onglet **Protection du courrier**.

ANALYSE DU COURRIER DANS THE BAT!

Les actions à réaliser sur les objets infectés des messages électroniques dans The Bat! sont définies par le programme en lui-même.

Les paramètres de l'Antivirus Courrier qui définissent l'analyse ou non du courrier entrant et sortant ainsi que les actions à réaliser sur les objets dangereux de messages et les exclusions sont ignorées. Le seul élément pris en considération par The Bat!, c'est l'analyse des archives jointes.

Les paramètres de la protection du courrier sont diffusés à tous les composants antivirus installés sur l'ordinateur compatibles avec The Bat!.

Il ne faut pas oublier que lors de la réception de messages, ceux-ci sont d'abord analysés par l'Antivirus Courrier, puis ensuite par le plug-in du client de messagerie The Bat!. Kaspersky Anti-Virus signalera la découverte d'un objet malveillant. Si dans la fenêtre de notification de l'Antivirus Courrier vous sélectionnez l'option **Réparer (Supprimer)**, les actions liées à la suppression de la menace seront exécutées par l'Antivirus Courrier. Si vous choisissez **Ignorer**, alors l'objet sera neutralisé par le plug-in de The Bat!. Lors de l'envoi de courrier, les messages sont d'abord analysés par le plug-in puis par l'Antivirus Courrier.

La configuration des paramètres de l'Antivirus Courrier depuis l'application The Bat! est accessible si cela est indiqué dans les paramètres de la zone d'analyse de l'Antivirus Courrier.

Pour configurer l'analyse du courrier dans The Bat!, vous devez définir les critères suivants :

- Le flux de messagerie qui sera soumis à l'analyse (courrier entrant, sortant) ;
- Le moment où il faudra analyser les objets du message (à l'ouverture du message, avant l'enregistrement sur le disque) ;
- Les actions exécutées par le client de messagerie en cas de découverte d'objets dangereux dans les messages électroniques. Vous pouvez par exemple choisir :
  - **Tenter de réparer les parties infectées** : quand cette option est sélectionnée, une tentative de réparation de l'objet sera lancée. Si elle échoue, l'objet restera dans le message.
  - **Supprimer les parties infectées** : quand cette option est sélectionnée, l'objet dangereux du message sera supprimé, qu'il soit infecté ou potentiellement infecté.

Par défaut, tous les objets infectés des messages sont placés en quarantaine par The Bat! sans réparation.

Les messages électroniques qui contiennent des objets dangereux ne sont pas différenciés par un titre spécial lors de l'analyse par le plug-in dans le client de messagerie The Bat!.

Pour configurer les paramètres de l'analyse du courrier dans l'application The Bat!, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application The Bat!.
2. Dans le menu **Propriétés**, sélectionnez l'option **Configuration**.
3. Dans l'arborescence des paramètres, choisissez l'objet **Protection contre les virus**.

ANTIVIRUS INTERNET

Chaque fois que vous utilisez Internet, vous exposez votre ordinateur et les données qu'il contient à un risque d'infection par des virus et par d'autres applications présentant une menace. Ils peuvent s'infiltrer dans votre ordinateur quand vous téléchargez les programmes gratuits ou quand vous consultez les informations sur les sites web qui ont été soumis à des attaques de pirates avant votre visite. De plus, les vers de réseau peuvent s'introduire sur votre ordinateur avant l'ouverture des pages Web ou le téléchargement d'un fichier, directement à l'ouverture de la connexion Internet.

L'Antivirus Internet protège les informations qui arrivent sur votre ordinateur et qui sont envoyées depuis celui-ci via les protocoles HTTP, HTTPS et FTP et empêche l'exécution de scripts dangereux sur l'ordinateur.

L'Antivirus Internet contrôle le trafic qui transite uniquement via les ports indiqués dans la liste des ports contrôlés. La liste des ports contrôlés le plus souvent utilisés pour le transfert de données est livrée avec Kaspersky Anti-Virus. Si vous utilisez des ports qui ne figurent pas dans la liste des ports contrôlés, ajoutez-les à cette liste (cf. section "Constitution de la liste des ports contrôlés" à la page 106) afin de garantir la protection du flux de données transitant par ceux-ci.

L'Antivirus Internet analyse le trafic conformément aux paramètres définis dans le niveau de protection. Quand l'Antivirus Internet découvre une menace, il exécute l'action définie. L'identification des objets malveillants est réalisée à l'aide des bases utilisées par Kaspersky Anti-Virus et d'un algorithme heuristique.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Internet. Dans la majorité des cas, il suffit de sélectionner le niveau de protection qui convient.

Algorithme d'analyse du trafic Web

Chaque page Web ou fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque via le protocole HTTP, HTTPS et FTP est intercepté et analysé par l'Antivirus Internet pour découvrir la présence éventuelle de code malveillant :

- Si la page Web ou le fichier que souhaite ouvrir l'utilisateur contient un code malveillant, l'accès est bloqué. Dans ce cas, un message apparaît à l'écran pour avertir l'utilisateur que le fichier ou la page web demandé est infecté.
- Si aucun code malveillant n'a été découvert dans le fichier ou la page Web, l'utilisateur pourra y accéder immédiatement.

Algorithme d'analyse des scripts

Chaque script lancé est intercepté par l'Antivirus Internet et soumis à la recherche d'un code malveillant éventuel :

- Si le script contient un code malveillant, l'Antivirus Internet le bloque et affiche une notification sur l'écran.

- Si le script ne contient aucun code malveillant, le script est exécuté.

L'Antivirus Internet intercepte uniquement les scripts basés sur la technologie Microsoft Windows Script Host.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS INTERNET

Par défaut, l'Antivirus Internet est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Internet le cas échéant.

Pour désactiver l'utilisation de l'Antivirus Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus Internet**.

MODIFICATION ET RESTAURATION DU NIVEAU DE PROTECTION DU TRAFIC INTERNET

En fonction des besoins actuels, vous pourrez choisir un des niveaux de protection prédéfinis pour la protection du courrier ou configurer vous-même les paramètres de fonctionnement de l'Antivirus Internet.

Sachez que si vous configurez les paramètres de fonctionnement de l'Antivirus Internet, vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Afin de modifier le niveau de protection du trafic Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans le groupe **Niveau de protection** de la partie droite de la fenêtre, sélectionnez le niveau de protection requis ou cliquez sur le bouton **Configuration** afin de définir manuellement les paramètres d'analyse.

   En cas de configuration manuelle, l'appellation du niveau de protection devient **Autre**.

Pour restaurer le niveau de protection du trafic Web par défaut, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans la partie droite de la fenêtre, dans le groupe **Niveau de protection**, cliquez sur **Par défaut**.

MODIFICATION DE L'ACTION SUR LES OBJETS DANGEREUX DU TRAFIC INTERNET

En cas de découverte d'objets infectés, l'application exécute l'action définie.

S'agissant des actions sur les scripts dangereux, l'Antivirus Internet bloque toujours leur exécution et affiche un message qui informe l'utilisateur sur l'action réalisée. La modification de l'action à effectuer sur un script dangereux n'est pas possible. Seule la désactivation de l'analyse des scripts (cf. section "Blocage des scripts dangereux" à la page 96) est autorisée.

Pour modifier l'action à effectuer sur les objets découverts, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans la partie droite de la fenêtre, dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'option requise.

ANALYSE DES LIENS SUR LES PAGES WEB

La recherche d'indicateurs d'hameçonnage (phishing) sur les pages Web permet d'éviter les *attaques d'hameçonnage (phishing)*. En général, une attaque d'hameçonnage (phishing) se déroule via des messages prétendument envoyés par des institutions financières et qui contiennent des liens vers les sites de ces organisations. Le texte du message invite le destinataire à cliquer sur le lien et à saisir des données confidentielles (numéro de carte de crédit ou données d'identification pour l'accès aux services bancaires en ligne) sur la page qui s'affiche. L'exemple type est le message envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que sa véritable adresse s'affiche alors que vous vous trouvez en fait sur un site fictif. Toutes vos actions sur ce site sont surveillées et pourraient servir au vol de votre argent.

Dans la mesure où le lien vers un site d'hameçonnage (phishing) peut figurer non seulement dans un courrier, mais également dans un message ICQ, l'Antivirus Internet contrôle les tentatives d'accès à un site d'hameçonnage (phishing) au niveau de l'analyse du trafic Web et bloque l'accès à ces sites Web.

Outre les bases de Kaspersky Anti-Virus, vous pouvez compter sur l'analyse heuristique (cf. page 95) pour identifier les traces d'hameçonnage (phishing) sur les pages Web.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE L'ANALYSE DES LIENS

Pour activer l'analyse des liens selon les bases des URL suspectes et la recherche d'hameçonnage (phishing), procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Sous l'onglet **Général** dans le groupe **Analyse des liens**, cochez les cases **Analyser les liens selon la base des URL suspectes** et **Vérifier si les pages appartiennent à un site d'hameçonnage (phishing)**.

UTILISATION DU MODULE D'ANALYSE DES LIENS

Le module d'analyse des liens est intégré aux navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome sous forme d'un plug-in.

Le module analyse tous les liens de la page Web ouverte sur l'appartenance aux adresses Web suspectes et sur la présence d'hameçonnage (phishing) et marque les liens par la couleur dans la fenêtre du navigateur.

Il est possible de former la liste des sites Web sur lesquels les liens seront analysés, d'analyser les liens sur tous les sites Web (sauf ceux de la liste des exclusions), d'analyser uniquement les liens dans les résultats de recherche, ainsi que d'indiquer les catégories des sites Web dont les liens doivent être analysés.

Il est possible de configurer le module d'analyse des liens non seulement dans la fenêtre de configuration de l'application, mais aussi dans la fenêtre de configuration du module accessible depuis le navigateur web.

Pour indiquer les sites Web sur lesquels il faut analyser les liens, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. La fenêtre **Antivirus Internet** s'ouvre.
5. Sous l'onglet **Filtrage de liens** dans le groupe **Analyse des liens (URL)**, cochez la case **Activer l'analyse des liens**.
6. sélectionnez les sites Web sur lesquels il faut vérifier les liens :

   a. Si vous voulez former la liste des sites Web sur lesquels il faut analyser les liens, sélectionnez l'option **Uniquement les sites Web de la liste** et cliquez sur le bouton **Sélection**. Dans la fenêtre ouverte **URL analysées**, formez la liste des sites Web analysés.

   b. Si vous voulez analyser les liens sur tous les sites Web, sauf les sites indiqués, sélectionnez l'option **Tous, sauf les exclusions** et cliquez sur le bouton **Exclusions**. Dans la fenêtre ouverte **Exclusions**, formez la liste des sites Web dont il ne faut pas analyser les liens.

Pour analyser les liens uniquement dans les résultats de recherche, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

4. La fenêtre **Antivirus Internet** s'ouvre.

5. Sous l'onglet **Filtrage de liens**, dans le groupe **Analyse des liens (URL Advisor)**, cochez la case **Activer l'analyse des liens** et cliquez sur le bouton **Configuration**.

6. Dans la fenêtre ouverte **Configuration du module d'analyse des liens** dans le groupe **Mode d'analyse**, sélectionnez l'option **Uniquement les liens dans les résultats de recherche**.

- *Pour sélectionner les catégories des sites Web dont les liens doivent être analysés, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

4. La fenêtre **Antivirus Internet** s'ouvre.

5. Sous l'onglet **Filtrage de liens**, dans le groupe **Analyse des liens (URL Advisor)**, cochez la case **Activer l'analyse des liens** et cliquez sur le bouton **Configuration**.

6. Dans la fenêtre ouverte **Configuration du module d'analyse des liens**, dans le groupe **Catégories de sites Web**, cochez la case **Afficher les informations sur les catégories du contenu des sites Web**.

7. Dans la liste des catégories, cochez les cases en regard des catégories des sites Web dont les liens doivent être analysés.

- *Pour ouvrir la fenêtre de configuration du module d'analyse des liens depuis la fenêtre du navigateur,*

cliquez sur le bouton avec l'icône de Kaspersky Anti-Virus dans la barre d'outils du navigateur.

UTILISATION DE L'ANALYSE HEURISTIQUE LORS DU FONCTIONNEMENT DE L'ANTIVIRUS INTERNET

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

Lors du fonctionnement de l'Antivirus Internet, il est possible d'activer, indépendamment les uns des autres, l'analyse heuristique pour analyser le trafic Web et l'analyse des pages Web concernant sur l'hameçonnage (phishing).

- *Pour activer l'analyse heuristique pour analyser le trafic Web, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Sous l'onglet **Général** dans le groupe **Analyse heuristique**, cochez la case **Activer l'analyse heuristique** et définissez le niveau de détail de l'analyse.

- *Pour activer l'analyse heuristique pour analyser les pages Web sur l'hameçonnage (phishing), procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Sous l'onglet **Général** dans le groupe **Analyse des liens**, cliquez sur le bouton **Avancé**.

5. Dans la fenêtre **Configuration de l'Anti-Phishing** qui s'ouvre, cochez la case **Utiliser l'analyse heuristique lors de la recherche d'éventuels liens d'hameçonnage (phishing) dans les pages Web** et définissez le niveau de détail de l'analyse.

BLOCAGE DES SCRIPTS DANGEREUX

L'Antivirus Internet analyse tous les scripts traités par Microsoft Internet Explorer ainsi que n'importe quel script WSH (JavaScript, Visual Basic Script, etc.) lancé pendant que l'utilisateur travaille sur l'ordinateur. Si le script constitue une menace pour l'ordinateur, son exécution sera bloquée.

Pour activer le blocage des scripts dangereux, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Sous l'onglet **Général** dans le groupe **Avancé**, décochez la case **Bloquer les scripts dangereux dans Microsoft Internet Explorer**.

OPTIMISATION DE L'ANALYSE

Afin d'augmenter l'efficacité de la détection des codes malveillants, l'Antivirus Internet utilise la technologie de mise en cache de fragments des objets envoyés via Internet. En utilisant la mise en cache, l'Antivirus Internet analyse les objets uniquement après qu'ils aient été entièrement reçus sur l'ordinateur.

Le recours à la mise en cache augmente la durée de traitement des objets et retarde leur transfert pour les manipulations. De plus, la mise en cache peut entraîner des problèmes lors du téléchargement et du traitement de grands objets en raison de l'expiration du délai d'attente de la connexion du client HTTP.

Pour résoudre ce problème, la possibilité de limiter la durée de la mise en cache des fragments des objets envoyés via Internet est prévue. Une fois le délai écoulé, chaque partie de l'objet reçue est transmise sans vérification et l'objet est analysé complètement une fois qu'il a été copié. Ceci permet d'accélérer le transfert de l'objet et de résoudre le problème de la déconnexion. Le niveau de protection de l'utilisation d'Internet ne sera pas réduit pour la cause.

La levée de la restriction sur la durée de la mise en cache du trafic Web améliore l'efficacité de l'analyse antivirus mais provoque en même temps un ralentissement de l'accès aux objets.

Pour limiter la durée de la mise en cache des fragments ou pour supprimer cette limite, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.

4. Sous l'onglet **Général** dans le groupe **Avancé**, cochez la case **Limiter la durée de mise en cache du trafic pour l'optimisation de l'analyse**.

COMPOSITION D'UNE LISTE D'ADRESSES DE CONFIANCE

L'Antivirus Internet n'analyse pas le trafic Web obtenu depuis les adresses de confiance sur la présence des objets dangereux.

Pour composer une liste d'URL de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Antivirus Internet** dans la section **Protection**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Sous l'onglet **Sites de confiance**, cochez la case **Ne pas analyser le trafic Internet en provenance des URL de confiance**.
5. Formez la liste des sites Web/pages Web dont vous considérez le contenu comme étant fiable. Pour ce faire, procédez comme suit :

   a. Cliquez sur le bouton **Ajouter**.

      La fenêtre **Masque d'adresse** s'ouvre.

   b. Saisissez l'adresse du site Web/de la page Web ou le masque d'adresse du site Web/de la page Web.

   c. Cliquez sur le bouton **OK**.

      Un nouvel enregistrement apparaîtra dans la liste des adresses Web de confiance.
6. Le cas échéant, répétez les points a – c de l'instruction.

ANTIVIRUS IM ("CHAT")

L'Antivirus IM est prévu pour analyser le trafic transmis par les *clients de messageries instantanées*.

Les messages transmis via les clients de messagerie instantanée peuvent contenir des liens vers des sites web suspects ou vers des sites web utilisés par les individus malintentionnés dans le cadre d'attaques d'hameçonnage (phishing). Les programmes malveillants utilisent les clients de messagerie instantanée pour diffuser des messages non sollicités ainsi que des liens vers des applications (voire les applications elles-mêmes) qui volent les numéros et les mots de passe des utilisateurs.

Kaspersky Anti-Virus garantit une utilisation sans danger des systèmes de messagerie instantanée tels qu'ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent et IRC.

Certains clients de messagerie instantanée, par exemple, Yahoo! Messenger et Google Talk utilisent une connexion sécurisée. Pour analyser le trafic de ces applications, il faut activer l'analyse des connexions cryptées (cf. page 104).

L'Antivirus IM intercepte les messages et analyse la présence d'objets ou de liens dangereux. Vous pouvez sélectionner les types de messages qu'il faut analyser et sélectionner les différentes méthodes d'analyse.

Quand il découvre une menace dans un message, l'Antivirus IM remplace le message par un avertissement pour l'utilisateur.

Les fichiers transmis par la messagerie instantanée sont analysés par l'Antivirus Fichiers (cf. page 79) pendant la tentative d'enregistrement.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS IM

Par défaut, l'Antivirus IM est activé et fonctionne en mode optimal. Vous pouvez désactiver l'Antivirus IM le cas échéant.

Pour désactiver l'utilisation de l'Antivirus IM, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus IM ("Chat")**.

FORMATION DE LA ZONE DE PROTECTION DE L'ANTIVIRUS IM

La zone de protection désigne les types de message qu'il faut analyser. Kaspersky Anti-Virus analyse par défaut aussi bien les messages entrant que les messages sortant. Si vous êtes convaincu que les messages que vous envoyez ne contiennent aucun objet dangereux, vous pouvez vous passer de l'analyse du trafic sortant.

Pour désactiver l'analyse des messages sortant, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
3. Sélectionnez l'option **Analyser uniquement le courrier entrant** dans le groupe **Zone de protection** de la partie droite de la fenêtre.

ANALYSE DES LIENS DANS LES MESSAGES ENVOYES PAR LES MESSAGERIES INSTANTANEES

Pour rechercher des liens suspects ou d'hameçonnage (phishing) dans les messages, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
3. Dans la partie droite de la fenêtre dans le groupe **Méthodes d'analyse**, cochez les cases **Analyser les liens selon la base des URL suspectes** et **Analyser les liens selon la base des URL d'hameçonnage (phishing)**.

UTILISATION DE L'ANALYSE HEURISTIQUE DANS L'ANTIVIRUS IM ("CHAT")

Pour augmenter l'efficacité de la protection, vous pouvez utiliser *l'analyse heuristique* (analyse de l'activité de l'objet dans le système). Cette analyse permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

Lors de l'analyse heuristique, n'importe quel script contenu dans les messages de client de messagerie instantanée est exécuté dans l'environnement protégé. Si l'activité du script est caractéristique des objets malveillants, alors l'objet peut être considéré, avec une probabilité élevée, comme un objet malveillant ou suspect. L'analyse heuristique est activée par défaut.

Pour activer l'utilisation de l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Antivirus IM ("Chat")**.
3. Cochez la case **Analyse heuristique** dans le groupe **Méthodes d'analyse** de la partie droite de la fenêtre.

DEFENSE PROACTIVE

La Défense Proactive protège l'ordinateur contre les nouvelles menaces dont les informations ne figurent pas encore dans les bases de Kaspersky Anti-Virus.

Le fonctionnement de la Défense Proactive est basé sur l'utilisation des technologies préventives. Ces technologies permettent de neutraliser une nouvelle menace avant qu'elle n'ait pu nuire à votre ordinateur. A la différence des technologies réactives qui réalisent l'analyse selon les enregistrements des bases de Kaspersky Anti-Virus, les technologies préventives identifient les nouvelles menaces en suivant les séquences d'actions exécutées par l'application. Si l'analyse de la séquence d'actions de l'application éveille des soupçons, Kaspersky Anti-Virus bloque l'activité de cette application.

Ainsi, si un programme se copie dans une ressource de réseau, dans le répertoire de démarrage et dans la base de registres, on peut affirmer sans crainte qu'il s'agit d'un ver.

Parmi les séquences d'actions dangereuses, nous pouvons citer également les tentatives de modification du fichier HOSTS, la dissimulation de l'installation de pilotes, etc. Vous pouvez néanmoins refuser de contrôler (cf. page 100) une activité dangereuse ou de modifier la règle de contrôle (cf. page 100).

Vous pouvez créer un groupe d'applications (cf. page 100) de confiance pour la Défense Proactive. Les notifications sur l'activité de ces applications ne seront pas affichées.

Si l'ordinateur tourne sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 ou Microsoft Windows 7 x64, certains événements ne seront pas contrôlés. Ceci est lié aux particularités des systèmes d'exploitation cités. Ainsi, l'envoi des données par les applications de confiance et l'activité suspecte dans le système ne seront pas complètement contrôlés.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE LA DEFENSE PROACTIVE

Par défaut, la Défense Proactive est activée et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Le cas échéant, vous pouvez désactiver la Défense Proactive.

Pour désactiver la Défense Proactive, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer la Défense Proactive**.

CONSTITUTION D'UN GROUPE D'APPLICATIONS DE CONFIANCE

Vous pouvez composer des groupes d'applications de confiance dont l'activité sera ignorée par la Défense Proactive. Les applications dotées d'une signature numérique et les applications figurant dans la base de Kaspersky Security Network sont reprises par défaut dans la catégorie des applications de confiance.

Pour configurer les paramètres de composition d'un groupe d'applications de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre dans le groupe **Applications de confiance** exécutez les actions suivantes :
   - Si vous voulez placer les applications qui possèdent une signature numérique contrôlée dans le groupe des applications de confiance, cochez la case **Avec une signature numérique (Editeurs connus)**.
   - Si vous voulez placer les applications figurant dans la base de Kaspersky Security Network dans le groupe des applications de confiance, cochez la case **Applications de confiance de la base Kaspersky Security Network**.

UTILISATION DE LA LISTE DES ACTIVITES DANGEREUSES

La liste des actions en rapport avec les activités dangereuses ne peut être modifiée. Mais il est possible de refuser de contrôler une activité dangereuse.

Pour refuser de contrôler une activité dangereuse, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Défense Proactive** qui s'ouvre, décochez la case située en regard du nom de l'activité dont vous refusez le contrôle.

MODIFICATION DE L'ACTION PAR RAPPORT A L'ACTIVITE DANGEREUSE DES APPLICATIONS

La liste des actions en rapport avec les activités dangereuses ne peut être modifiée. Mais il est possible de modifier les actions exécutées par Kaspersky Anti-Virus lors de la détection d'une activité dangereuse de l'application.

Pour modifier l'action par rapport à l'activité dangereuse de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Défense Proactive** qui s'ouvre, dans la colonne **Evènement**, sélectionnez l'événement pour lequel la règle doit être modifiée.
5. Pour l'événement sélectionné, configurez les paramètres nécessaires de la règle à l'aide des liens dans le bloc de **Description de la règle**. Par exemple :
   a. Cliquez sur le lien indiquant l'action établie et dans la fenêtre **Sélectionner une action** ouverte, sélectionnez l'action nécessaire parmi les actions proposées.
   b. Cliquez sur le lien **Act./Désact.**, pour indiquer la nécessité de créer un rapport sur l'opération exécutée.

SURVEILLANCE DE L'ACTIVITE

La Surveillance de l'activité récolte des données sur l'activité des applications concernant l'ordinateur et partage ces informations aux autres composants afin qu'ils puissent offrir une protection plus efficace.

Sur la base des informations collectées par Surveillance du système, Kaspersky Anti-Virus peut revenir à l'état antérieur aux actions réalisées par les applications malveillantes.

La remise à l'état antérieur des actions de l'application malveillante peut être initiée par un des composants suivants de la protection :

- Surveillance de l'activité sur la base de modèles de comportement dangereux ;
- Défense Proactive ;
- Antivirus Fichiers ;
- Pendant la recherche de virus.

Lorsque les composants de la protection de Kaspersky Anti-Virus découvrent des événements suspects dans le système, ils peuvent demander des informations complémentaires à la Surveillance de l'activité. En cas d'utilisation de Kaspersky Anti-Virus en mode interactif (cf. section "Sélection du mode de protection" à la page 64), vous pouvez consulter les données collectées par le composant Surveillance du système sous forme de rapport sur l'historique de l'activité dangereuse. Ces données permettent de prendre une décision lors du choix de l'action dans la fenêtre de notification. Ainsi, lors de la détection du programme malveillant par le composant, un lien vers le rapport de la Surveillance de l'activité apparaît dans la partie supérieure de la fenêtre des notifications (cf. page 151) et propose une action.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE LA SURVEILLANCE DE L'ACTIVITE

Par défaut, la Surveillance du système est activée et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Le cas échéant, vous pouvez activer la Surveillance du système.

Il est déconseillé de désactiver le composant sans raison car cela réduirait l'efficacité du fonctionnement de la Défense Proactive et du Contrôle des Applications, ainsi que d'autres composants de la protection qui peuvent demander les données récoltées par la Surveillance de l'activité pour préciser la menace potentielle détectée.

Pour désactiver l'utilisation de la Surveillance de l'activité, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Surveillance du système**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer le Surveillance du système**.

UTILISATION DES MODELES DE COMPORTEMENT DANGEREUX (BSS)

Les modèles de comportement dangereux (BSS, Behavior Stream Signatures) contiennent la séquence d'actions d'applications considérées comme dangereuses. Lorsque l'activité d'une application correspond à un des modèles de comportement dangereux, Kaspersky Anti-Virus exécute l'action définie.

Afin d'offrir une protection efficace, Kaspersky Anti-Virus dispose de modèles de comportement dangereux utilisés par la Surveillance du système pendant la mise à jour des bases.

Par défaut, en cas d'utilisation de Kaspersky Anti-Virus en mode automatique, si l'activité de l'application correspond à un modèle de comportement dangereux, la Surveillance du système place cette application en quarantaine et en mode interactif, et demande à l'utilisateur de confirmer l'action. Vous pouvez indiquer l'action à exécuter quand l'activité d'une application correspond à un modèle de comportement dangereux.

Outre les équivalences exactes entre l'activité d'une application et les modèles de comportement dangereux, la Surveillance de l'activité découvre les actions qui correspondent en partie aux modèles de comportement dangereux et qui sont suspectes, suite à l'analyse heuristique. En cas de découverte d'une activité suspecte, la Surveillance du système demande à l'utilisateur de confirmer l'action, quel que soit le mode de fonctionnement.

Pour sélectionner l'action à exécuter en cas de correspondance entre l'activité d'une application et un modèle de comportement dangereux, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Surveillance du système**.
3. Dans la partie droite de la fenêtre, dans le groupe **Analyse heuristique**, cochez la case **Utiliser les modèles de comportement dangereux (BSS) actualisés**.
4. Sélectionnez l'option **Exécuter l'action**, puis choisissez l'action requise dans la liste déroulante.

RETOUR A L'ETAT ANTERIEUR AUX ACTIONS DU PROGRAMME MALVEILLANT

Vous pouvez utiliser la fonction du rétablissement du système à l'état antérieur aux actions du programme malveillant. Pour pouvoir revenir à l'état antérieur, la Surveillance du système conserve l'historique de l'activité des applications. Il est possible de limiter le volume des données que la Surveillance du système conserve pour le retour à l'état antérieur.

Par défaut, lorsque Kaspersky Anti-Virus fonctionne en mode automatique, le retour à l'état antérieur s'opère automatiquement lorsque les composants de la protection découvrent une activité malveillante. En mode interactif, la Surveillance du système demande à l'utilisateur de confirmer l'action. Vous pouvez désigner l'action à exécuter en cas de découverte d'une possibilité de retour à l'état antérieur des actions de l'application malveillante.

Le retour à l'état antérieur aux actions du programme malveillant touche un ensemble de données clairement délimité. Cette procédure n'a aucun impact négatif sur le fonctionnement du système d'exploitation, ni sur l'intégrité des informations enregistrées sur l'ordinateur.

- *Pour sélectionner l'action en cas de découverte d'une possibilité de retour à l'état antérieur des actions de l'application malveillante, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Surveillance du système**.
  3. Dans la partie droite de la fenêtre dans le groupe **Remise à l'état antérieur des actions de l'application malveillante**, sélectionnez l'option **Exécuter l'action**, puis sélectionnez l'action nécessaire dans la liste déroulante.

- *Pour limiter le volume des données que la Surveillance du système conserve pour le retour à l'état antérieur, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.
  2. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le composant **Surveillance du système**.
  3. Dans la partie droite de la fenêtre dans le groupe **Remise à l'état antérieur des actions de l'application malveillante**, cochez la case **Limiter le volume des informations enregistrées pour la remise** et indiquer le volume maximal des données que la Surveillance du système conservera pour le retour à l'état antérieur.

PROTECTION DU RESEAU

Les différents outils et les paramètres de Kaspersky Anti-Virus garantissent la protection et le contrôle de votre utilisation du réseau.

Les sections suivantes contiennent des informations détaillées sur l'analyse des connexions cryptées, les paramètres du serveur proxy et le contrôle des ports de réseau.

DANS CETTE SECTION

ANALYSE DES CONNEXIONS SECURISEES

Les connexions à l'aide des protocoles SSL/TLS protègent le canal d'échange des données sur Internet. Les protocoles SSL/TLS permettent d'identifier les parties qui échangent les données sur la base de certificats électroniques, de crypter les données transmises et de garantir leur intégrité tout au long de la transmission.

Ces particularités du protocole sont exploitées par les individus malintentionnés afin de diffuser leurs logiciels malveillants car la majorité des logiciels antivirus n'analyse pas le trafic SSL/TLS.

Kaspersky Anti-Virus analyse les connexions cryptées à l'aide d'un certificat de Kaspersky Lab.

Si un certificat non valide est découvert au moment d'établir la connexion avec le serveur (par exemple, il a été remplacé par un individu malintentionné), un message s'affichera et invitera l'utilisateur à accepter ou non le certificat.

Si vous êtes certain que la connexion au site ne constituera jamais une menace, même si le certificat n'est pas correct, vous pouvez l'ajouter à la liste des adresses de confiance. Kaspersky Anti-Virus n'analysera plus à l'avenir la connexion sécurisée avec ce site.

Vous pouvez utiliser l'Assistant d'installation du certificat pour installer le certificat d'analyse des connexions cryptées en mode semi-automatique dans les navigateurs Microsoft Internet Explorer, Mozilla Firefox (s'il n'est pas lancé) et Google Chrome ainsi que pour obtenir des instructions sur l'installation du certificat de Kaspersky Lab pour le navigateur Opera.

Pour activer l'analyse des connexions cryptées et installer le certificat de Kaspersky Lab, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez le composant **Réseau** dans la section **Paramètres avancés**.
3. Dans la fenêtre qui s'ouvre, cochez la case **Analyse des connexions sécurisées**. Quand ce paramètre est activé pour la première fois, l'Assistant d'installation du certificat est lancé automatiquement.
4. Si l'Assistant ne démarre pas, cliquez sur **Installer le certificat**. Cette action lance un Assistant dont il faudra suivre les indications pour l'installation du certificat de Kaspersky Lab.

DANS CETTE SECTION

ANALYSE DES CONNEXIONS CRYPTEES DANS MOZILLA FIREFOX

Le navigateur Mozilla Firefox n'utilise pas le référentiel des certificats de Microsoft Windows. Pour analyser les connexions cryptées à l'aide de Firefox, il faut installer manuellement le certificat de Kaspersky Lab.

Vous pouvez également utiliser l'Assistant d'installation du certificat si le navigateur n'est pas lancé.

Pour installer manuellement le certificat de Kaspersky Lab, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Dans le groupe **Certificats**, sélectionnez l'onglet **Sécurité** et cliquez sur **Voir le certificat**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification**, puis cliquez sur le bouton **Restaurer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur **Voir**.

Pour installer manuellement le certificat de Kaspersky Lab pour Mozilla Firefox version 3.x, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.

2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

3. Sous l'onglet **Cryptage**, cliquez sur **Voir le certificat**.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification** puis cliquez sur le bouton **Importer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur **Voir**.

Si votre ordinateur fonctionne sous le système d'exploitation Microsoft Windows Vista ou Microsoft Windows 7, alors le chemin d'accès au fichier du certificat de Kaspersky Lab sera :
%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

ANALYSE DES CONNEXIONS CRYPTEES DANS OPERA

Le navigateur Opera n'utilise pas le référentiel de certificats de Microsoft Windows. Pour analyser les connexions cryptées à l'aide d'Opera, il faut installer manuellement le certificat de Kaspersky Lab.

Pour installer le certificat de Kaspersky Lab, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.

2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Editeurs**, puis cliquez sur le bouton **Importer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé. Pour consulter les informations relatives au certificat et pour sélectionner les actions qui utiliseront le certificat, sélectionnez le certificat dans la liste et cliquez sur le bouton **Voir**.

Pour installer le certificat de Kaspersky Lab pour Opera version 9.x, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez l'option **Outils** → **Configuration**.

2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certification** puis cliquez sur le bouton **Importer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé.

Si votre ordinateur fonctionne sous le système d'exploitation Microsoft Windows Vista et Microsoft Windows 7, alors le chemin d'accès au fichier du certificat de Kaspersky Lab sera :
%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

CONFIGURATION DES PARAMETRES DU SERVEUR PROXY

Si la connexion à Internet s'opère via un serveur proxy, il faudra alors peut-être configurer les paramètres de connexion à ce dernier. Kaspersky Anti-Virus applique ces paramètres à quelques composants de la protection ainsi qu'à la mise à jour des bases et des modules de l'application.

Si votre réseau est doté d'un serveur proxy qui utilise un port inhabituel, il faudra l'ajouter à la liste des ports contrôlés (cf. section "Constitution de la liste des ports contrôlés" à la page 106).

Pour configurer les paramètres de connexion au serveur proxy, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez le composant **Réseau** dans la section **Paramètres avancés**.

3. Dans le groupe **Serveur proxy**, cliquez sur le bouton **Paramètres du serveur proxy**.

4. Dans la fenêtre ouverte **Paramètres du serveur proxy** définissez les paramètres de connexion au serveur proxy.

CONSTITUTION DE LA LISTE DES PORTS CONTROLES

Les composants de la protection tels que l'Antivirus Courrier, l'Antivirus Internet et l'Antivirus IM ("Chat") (cf. page 91) contrôlent les flux de données transmis par des protocoles définis et qui transitent par certains ports TCP ouverts de l'ordinateur. Ainsi par exemple, Antivirus Courrier analyse les informations transmises via le protocole SMTP et Antivirus Internet, les informations transmises via les protocoles HTTP, HTTPS et FTP.

Vous pouvez activer le contrôle de tous les ports de réseau ou des ports sélectionnés uniquement. Dans le cadre du contrôle des ports sélectionnés, vous pouvez composer une liste d'applications pour lesquelles il faudra contrôler tous les ports. Il est conseillé d'inclure dans cette liste les applications qui reçoivent ou transmettent des données via FTP.

Pour ajouter un port à la liste des ports contrôlés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, choisissez la sous-section **Réseau** dans la section **Paramètres avancés**.

3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports sélectionnés**, puis cliquez sur le bouton **Sélectionner**.

   La fenêtre **Ports de réseau** s'ouvre.

4. Le lien **Ajouter**, situé sous la liste des ports dans la partie supérieure de la fenêtre, ouvre la fenêtre **Port de réseau** dans laquelle vous pouvez saisir le numéro du port et une description.

Pour exclure un port à la liste des ports contrôlés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-section **Réseau** dans la section **Paramètres avancés**.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports sélectionnés**, puis cliquez sur le bouton **Sélectionner**.

   La fenêtre **Ports de réseau** s'ouvre.
4. Dans la liste des ports de la partie supérieure de la fenêtre, décochez la case en regard de la description du port qu'il faut exclure.

Pour composer la liste des applications dont l'ensemble des ports devra être analysé, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-section **Réseau** dans la section **Paramètres avancés**.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports sélectionnés**, puis cliquez sur le bouton **Sélectionner**.

   La fenêtre **Ports de réseau** s'ouvre.
4. Cochez la case **Contrôler tous les ports pour les applications indiquées** et dans la liste des applications en dessous, cochez les cases en regard des noms des applications pour lesquelles il faut contrôler tous les ports.
5. Si l'application nécessaire ne figure pas dans la liste, ajoutez-la d'une des manières suivantes :

   a. Le lien **Ajouter** situé sous la liste des applications ouvre le menu et permet de sélectionner une des options :

      - Pour indiquer l'emplacement du fichier exécutable de l'application, sélectionnez l'option **Parcourir** et indiquez l'emplacement du fichier sur l'ordinateur.
      - Pour sélectionner l'application dans la liste des applications en cours d'exécution, sélectionnez l'option **Applications**. Dans la fenêtre ouverte **Sélection de l'application**, sélectionnez l'application requise.

   b. Dans la fenêtre **Application** qui s'ouvre, saisissez une description de l'application sélectionnée.

ZONE DE CONFIANCE

La *zone de confiance* est une liste d'objets ignorés par l'application. En d'autres termes, il s'agit d'un ensemble d'exclusions de la protection de Kaspersky Anti-Virus.

La zone de confiance est composée sur la base de la liste des applications de confiance (cf. section "Composition de la liste des applications de confiance" à la page 108) et des règles d'exclusion (cf. section "Création de règles d'exclusion" à la page 109) en fonction des particularités des objets avec lesquels vous travaillez et des applications installées sur l'ordinateur. Il faudra peut-être inclure des objets dans la zone de confiance si Kaspersky Anti-Virus bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), ajoutez l'application Bloc-notes à la liste des applications de confiance afin d'exclure de l'analyse les objets qui utilisent ce processus.

De plus, certaines actions jugées dangereuses peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Ainsi, l'interception des frappes au clavier est une action standard pour les programmes de permutation automatique de la disposition du clavier (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

Quand une application est ajoutée à la liste des applications de confiance, l'activité de fichier et de réseau de celle-ci ne sera pas contrôlée (même les activités suspectes), ni les requêtes adressées à la base de registres système. Le fichier exécutable et le processus de l'application de confiance seront toujours soumis à la recherche de virus. Pour exclure entièrement l'application de l'analyse, il faut recourir aux règles d'exclusion.

Le recours aux exclusions d'applications de confiance de l'analyse permet de résoudre les éventuels problèmes de compatibilité entre Kaspersky Anti-Virus et d'autres applications (par exemple, le problème de la double analyse du trafic de réseau d'un ordinateur tiers par Kaspersky Anti-Virus et une autre application antivirus) et d'augmenter les performances de l'ordinateur, ce qui est particulièrement important en cas d'utilisation d'applications de serveur.

A leur tour, les règles d'exclusion de la zone de confiance permettent d'utiliser des applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et à vos données. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais elles pourraient être utilisées en guise d'auxiliaire pour un programme malveillant. Cette catégorie reprend les applications d'administration à distance, les clients IRC, les serveurs FTP, divers utilitaires de suspension ou d'arrêt de processus, les enregistreurs de frappe, les applications d'identification de mots de passe, les numéroteurs automatiques, etc. Kaspersky Anti-Virus peut bloquer de telles applications. Pour éviter le blocage, il est possible de créer des règles d'exclusion de l'analyse pour les applications utilisées.

La *règle d'exclusion* est un ensemble de conditions qui, si elles sont vérifiées, entraîne l'exclusion de l'objet de l'analyse réalisée par Kaspersky Anti-Virus. Dans tous les autres cas, l'analyse de l'objet en question sera réalisée par tous les composants de la protection conformément aux paramètres de protection définis pour ceux-ci.

Les règles d'exclusion de la zone de confiance peuvent être utilisées par plusieurs composants de la protection (par exemple, l'Antivirus Fichiers (cf. section "Antivirus Fichiers" à la page 79), l'Antivirus Courrier (cf. section "Antivirus Courrier" à la page 85), l'Antivirus Internet (cf. section "Antivirus Internet" à la page 91)), ou lors de l'exécution de tâches d'analyse.

DANS CETTE SECTION

COMPOSITION DE LA LISTE DES APPLICATIONS DE CONFIANCE

Par défaut Kaspersky Anti-Virus analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Quand une application est ajoutée à la liste des applications de confiance, Kaspersky Anti-Virus l'exclut de l'analyse.

Pour ajouter une application à la liste des applications de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Menaces et exclusions**.
3. Dans la section **Exclusions**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Applications de confiance**, ouvrez le menu de sélection de l'application à l'aide du bouton **Ajouter**.
5. Dans le menu déroulant, choisissez l'application dans la liste **Applications** ou sélectionnez l'option **Parcourir** pour indiquer le chemin d'accès au fichier exécutable de l'application souhaitée.
6. Dans la fenêtre **Exclusions pour l'application** qui s'ouvre, cochez les cases en regard des types d'activité de l'application qu'il ne faut pas analyser.

CREATION DE REGLES D'EXCLUSION

Si vous utilisez des applications que Kaspersky Anti-Virus considère légitimes mais qui pourraient être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou à vos données, il est conseillé de configurer des règles d'exclusion pour celles-ci.

Pour créer une règle d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Menaces et exclusions**.
3. Dans la section **Exclusions**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles d'exclusion**, cliquez sur le bouton **Ajouter**.
5. Dans la fenêtre **Règle d'exclusion** qui s'ouvre, définissez les paramètres de la règle d'exclusion.

PERFORMANCES ET COMPATIBILITE AVEC D'AUTRES APPLICATIONS

Dans le contexte de Kaspersky Anti-Virus, les performances désignent le spectre des menaces détectées ainsi que la consommation d'énergie et l'utilisation des ressources de l'ordinateur.

Kaspersky Anti-Virus permet de sélectionner diverses catégories de menaces (cf. section "Sélection des catégories de menaces identifiées" à la page 110) que l'application découvrira durant son fonctionnement.

Dans le cadre de l'utilisation d'un ordinateur portable, la consommation en énergie des applications est un élément particulièrement important. En particulier, la recherche d'éventuels virus sur l'ordinateur et la mise à jour des bases de Kaspersky Anti-Virus requièrent des ressources importantes. Le mode spécial de fonctionnement de Kaspersky Anti-Virus sur un ordinateur portable (cf. section "Economie d'énergie en cas d'alimentation via la batterie" à la page 110) permet de reporter automatiquement l'exécution des tâches d'analyse et de mise à jour programmées en cas d'alimentation via la batterie, ce qui permet d'économiser la charge de cette dernière, et le mode Analyse pendant les temps morts de l'ordinateur (cf. section "Lancement des tâches en arrière-plan" à la page 111) permet de lancer les tâches à forte intensité de ressources quand l'ordinateur n'est pas utilisé.

L'utilisation des ressources de l'ordinateur par Kaspersky Anti-Virus peut avoir un effet sur les performances des autres applications. Pour résoudre les problèmes liés au fonctionnement simultané en cas d'augmentation de la charge du processeur et des sous-système de disque, Kaspersky Anti-Virus suspend l'exécution des tâches d'analyse et cède des ressources aux autres applications (cf. section "Répartition des ressources de l'ordinateur pendant la recherche de virus" à la page 111) qui tournent sur l'ordinateur.

En Mode Jeux (cf. page 112), l'affichage des notifications sur le fonctionnement de Kaspersky Anti-Virus est automatiquement désactivé quand les autres applications sont lancées en mode plein écran.

La procédure de désinfection avancée en cas d'infection active du système requiert le redémarrage de l'ordinateur, ce qui peut également avoir un effet sur le fonctionnement des autres applications. Le cas échéant, vous pouvez suspendre l'application de la technologie de réparation d'une infection active (cf. page 110) afin d'éviter le redémarrage inopportun de l'ordinateur.

DANS CETTE SECTION

SELECTION DES CATEGORIES DE MENACES IDENTIFIEES

Les menaces qui peuvent être découvertes par Kaspersky Anti-Virus sont réparties en différentes catégories selon diverses caractéristiques. L'application détecte toujours les virus, les chevaux de Troie et les utilitaires malveillants. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Pour garantir une plus grande sécurité à l'ordinateur, il est possible d'élargir la liste de menaces découvertes en activant le contrôle des actions des applications légitimes qui pourraient être utilisées par un individu malintentionné pour nuire à l'ordinateur ou à vos données.

Pour sélectionner les catégories de menaces à identifier, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Menaces et exclusions**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration** situé sous la liste **Détection des menaces suivantes activée**.
4. Dans la fenêtre **Menaces** qui s'ouvre, cochez la case en regard de la catégorie de menace qu'il faut détecter.

ECONOMIE D'ENERGIE EN CAS D'ALIMENTATION VIA LA BATTERIE

Afin d'économiser les batteries des ordinateurs portables, vous pouvez reporter l'exécution des tâches d'analyse antivirus et de mises à jour programmées. Le cas échéant, il est possible d'actualiser Kaspersky Anti-Virus ou de lancer la recherche de virus manuellement.

Pour activer le mode d'économie d'énergie en cas d'alimentation via la batterie, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Economie d'énergie**.
3. Dans la partie droite de la fenêtre, cochez la case **Ne pas lancer l'analyse programmée en cas d'alimentation via la batterie**.

REPARATION DE L'INFECTION ACTIVE

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. En cas de découverte d'une action malveillante dans le système, Kaspersky Anti-Virus propose l'utilisation de la technologie de réparation de l'infection active qui permet de neutraliser la menace ou de la supprimer de l'ordinateur.

A la fin de la réparation de l'infection active, l'application exécute le redémarrage obligatoire de l'ordinateur. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète (cf. section "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page 48).

Pour que Kaspersky Anti-Virus applique la technologie de réparation de l'infection active, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Compatibilité**.
3. Cochez la case **Appliquer la technologie de réparation de l'infection active**.

REPARTITION DES RESSOURCES DE L'ORDINATEUR PENDANT LA RECHERCHE DE VIRUS

L'exécution des tâches d'analyse augmente la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, Kaspersky Anti-Virus arrête par défaut l'exécution des tâches d'analyse et libère des ressources pour les applications de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas du fonctionnement de tels programmes, il ne faut pas leur céder des ressources.

Pour que Kaspersky Anti-Virus reporte l'exécution des tâches d'analyse lorsque le fonctionnement des autres applications ralentit, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Compatibilité**.
3. Cochez la case **Céder les ressources aux autres applications**.

LANCEMENT DES TACHES EN ARRIERE-PLAN

Pour optimiser la charge sur les ressources de l'ordinateur, Kaspersky Anti-Virus réalise la recherche régulière d'outils de dissimulation d'activité en arrière plan et lance les tâches gourmandes en ressources quand l'ordinateur est en mode veille.

La recherche périodique des rootkits s'exécute pendant que vous utilisez votre ordinateur. La recherche dure pas plus de 5 minutes et utilise les ressources minimales de l'ordinateur.

Les tâches suivantes peuvent être exécutées pendant les temps morts de l'ordinateur :

- la mise à jour automatique des bases antivirus et des modules d'application ;
- l'analyse de la mémoire système, de la section système et des objets de démarrage.

Les tâches pendant les temps morts de l'ordinateur s'activent quand l'ordinateur est verrouillé par l'utilisateur ou si l'économiseur d'écran fonctionne pendant 5 minutes.

Lors du fonctionnement de l'ordinateur via la batterie, les tâches pendant les temps morts de l'ordinateur ne seront pas exécutées.

Après le lancement des tâches en arrière-plan, leur exécution s'affiche dans le Gestionnaire de tâches (cf. section "Administration des tâches d'analyse. Gestionnaire de tâches" à la page 73).

DANS CETTE SECTION

RECHERCHE D'OUTILS DE DISSIMULATION D'ACTIVITE EN ARRIERE PLAN

Kaspersky Anti-Virus réalise la recherche régulière d'outils de dissimulation d'activité par défaut. Le cas échéant, vous pouvez désactiver la recherche d'outils de dissimulation d'activité.

Pour désactiver la recherche régulière d'outils de dissimulation d'activité, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Analyse de l'ordinateur**, choisissez la sous-section **Paramètres généraux**.
3. Cochez la case **Exécuter la recherche régulière d'outils de dissimulation d'activité** dans la partie droite de la fenêtre.

ANALYSE EN MODE VEILLE DE L'ORDINATEUR

L'analyse de l'actualité des bases et des modules d'application est la première étape de lancement des tâches en mode veille de l'ordinateur. Si une mise à jour est requise selon les résultats de l'analyse, la tâche de la mise à jour automatique se lance. La date et l'état de la dernière exécution de la tâche en mode veille de l'ordinateur est vérifié à la deuxième étape. Si la tâche en mode veille de l'ordinateur n'était pas lancée, exécutée 7 jours avant pour la dernière fois ou suspendue, alors la tâche d'analyse de la mémoire système, du registre de système et des objets de démarrage est lancée.

L'analyse de l'ordinateur en mode veille est exécutée avec le niveau profond de l'analyse heuristique. Ce niveau augmente la probabilité de découverte des menaces masquées.

Quand l'utilisateur revient à son ordinateur, la tâche exécutée en mode veille est automatiquement interrompue. L'étape où l'analyse de l'ordinateur a été interrompue est mémorisée et la prochaine tâche reprendra à ce point.

Si l'exécution de tâches en mode veille de l'ordinateur est interrompue pendant le téléchargement des mises à jour, la mise à jour reprendra à zéro la prochaine fois.

Pour désactiver l'exécution de tâches pendant que l'ordinateur est en veille, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Analyse de l'ordinateur**, choisissez la sous-section **Paramètres généraux**.
3. Dans la partie droite de la fenêtre, décochez la case **Réaliser l'analyse en mode veille de l'ordinateur**.

UTILISATION EN MODE PLEIN ECRAN. MODE JEUX

L'utilisation de certaines applications (principalement des jeux) en mode plein écran peut créer des problèmes avec certaines fonctionnalités de Kaspersky Anti-Virus : par exemple, les fenêtres de notification n'ont pas leur place dans ce mode. Bien souvent, ces applications requièrent également des ressources considérables du système et c'est la raison pour laquelle l'exécution de certaines tâches de Kaspersky Anti-Virus peut ralentir ces applications.

Pour ne pas devoir désactiver manuellement les notifications ou suspendre les tâches chaque fois que vous utilisez le mode plein écran, Kaspersky Anti-Virus permet de modifier temporairement les paramètres grâce au mode Jeux. Quand

le Mode Jeux est utilisé, les paramètres de tous les composants sont automatiquement modifiés quand l'utilisateur passe en mode plein écran afin de garantir le fonctionnement optimal dans ce mode. Au moment de quitter le mode plein écran, les paramètres de l'application reprennent les valeurs en vigueur au moment de passer en mode plein écran.

Pour activer le mode jeu, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Mode Jeux**.
3. Cochez la case **Utiliser le Mode Jeux** et dans le groupe **Paramètres du profil** en dessous, définissez les paramètres indispensables de l'utilisation du Mode Jeux.

AUTODEFENSE DE KASPERSKY ANTI-VIRUS

Dans la mesure où Kaspersky Anti-Virus protège les ordinateurs contre les programmes malveillants, ceux-ci tentent, une fois qu'ils se sont infiltrés dans l'ordinateur, de bloquer le fonctionnement de Kaspersky Anti-Virus, voire de supprimer l'application de l'ordinateur.

La stabilité du système de protection de l'ordinateur est garantie par des mécanismes d'autodéfense et de protection contre l'interaction à distance intégrés à Kaspersky Anti-Virus.

L'autodéfense de Kaspersky Anti-Virus empêche la modification et la suppression des fichiers de l'application sur le disque, des processus dans la mémoire et des enregistrements dans la base de registres. La protection contre l'administration externe permet de bloquer toutes les tentatives d'administration à distance des services de l'application.

Sous les systèmes d'exploitation 64 bits et sous Microsoft Windows Vista, seule l'administration du mécanisme d'autodéfense de Kaspersky Anti-Virus contre la modification et la suppression de ses propres fichiers sur le disque ou contre la modification ou la suppression des clés dans la base de registres est accessible.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE L'AUTODEFENSE

L'autodéfense de Kaspersky Anti-Virus est activée par défaut. Le cas échéant, vous pouvez désactiver l'autodéfense.

Pour désactiver l'autodéfense de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-section **Autodéfense** dans la section **Paramètres avancés**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Autodéfense**.

PROTECTION CONTRE L'ADMINISTRATION EXTERNE

La protection contre l'administration externe est activée par défaut. Le cas échéant, vous pouvez désactiver cette protection.

Il arrive souvent qu'il faille utiliser une application d'administration à distance (par exemple, RemoteAdmin) alors que la protection contre l'administration externe est activée. Pour garantir leur fonctionnement, il faut ajouter ces applications à la liste des applications de confiance (cf. section "Zone de confiance" à la page 107) et activer le paramètre **Ne pas surveiller l'activité de l'application**.

Pour désactiver la protection contre l'administration externe, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-section **Autodéfense** dans la section **Paramètres avancés**.
3. Dans le groupe **Administration externe**, cochez la case **Interdire l'administration externe du service système**.

QUARANTAINE ET SAUVEGARDE

La *Quarantaine* est un référentiel spécial qui héberge les fichiers potentiellement infectés par des virus ou les fichiers qui ne peuvent être réparés au moment de la découverte.

L'objet potentiellement infecté peut être identifié et mis en quarantaine pendant l'analyse ainsi que par l'Antivirus Fichiers, l'Antivirus Courrier ou la Défense Proactive.

Les fichiers sont placés en quarantaine dans les cas suivants :

- Le code du fichier est semblable à celui d'une menace connue mais il a été partiellement modifié ou sa structure évoque celle d'un programme malveillant, mais ne figure pas dans la base. Dans ce cas, le fichier est placé en quarantaine suite à l'analyse heuristique pendant l'intervention de l'Antivirus Fichiers et de l'Antivirus Courrier, ainsi que pendant la recherche de virus. Le mécanisme d'analyse heuristique provoque rarement de faux positifs.
- La séquence d'actions réalisée par l'objet est suspecte. Dans ce cas, le fichier est placé en quarantaine suite à l'analyse de son comportement par la Défense Proactive.

Les fichiers mis en quarantaine ne représentent aucun danger. Avec le temps, les informations sur les nouvelles menaces et les modes de leur réparation apparaissent, et il est possible, Kaspersky Anti-Virus pourra réparer le fichier qui se trouve en quarantaine.

La *Sauvegarde* est prévue pour la conservation des copies de sauvegarde des fichiers supprimés ou modifiés pendant la réparation.

DANS CETTE SECTION

CONSERVATION DES FICHIERS EN QUARANTAINE ET DANS LA SAUVEGARDE

La durée maximale de conservation par défaut des objets est de 30 jours. Les objets sont supprimés à l'issue de cette période. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

En outre, vous pouvez indiquer la taille maximale de la quarantaine et de la sauvegarde. Une fois que la taille maximale est atteinte, le contenu de la quarantaine et de la sauvegarde est remplacé par de nouveaux objets. Par défaut, il n'y a pas de limite sur la taille maximale.

Pour configurer la durée maximale de conservation des objets, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Rapports et stockages**.
3. Dans la partie droite de la fenêtre, dans le groupe **Conservation des objets de la quarantaine et de la sauvegarde**, cochez la case **Supprimer les objets après** et indiquez la durée maximale de conservation des objets en quarantaine.

Pour configurer la taille maximale de la quarantaine ou de la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Rapports et stockages**.
3. Dans la partie droite de la fenêtre, dans le groupe **Conservation des objets de la quarantaine et de la sauvegarde**, cochez la case **Taille maximale** et indiquez la taille maximale de la quarantaine et de la sauvegarde.

MANIPULATION DES FICHIERS EN QUARANTAINE

La quarantaine de Kaspersky Anti-Virus permet d'exécuter les opérations suivantes :

- Mettre en quarantaine les fichiers qui selon vous sont infectés par un virus ;
- Analyser les fichiers en quarantaine à l'aide de la version actuelle des bases de Kaspersky Anti-Virus ;
- Restaurer les fichiers dans les dossiers où ils se trouvaient avant la mise en quarantaine ;
- Supprimer les fichiers sélectionnés de la quarantaine ;
- Envoyer les fichiers en quarantaine à Kaspersky Lab pour analyse.

Vous pouvez mettre un fichier en quarantaine d'une des méthodes suivantes :

- Via le bouton **Placer en quarantaine** dans la fenêtre **Quarantaine** ;
- Via le menu contextuel du fichier.

Pour placer le fichier en quarantaine depuis la fenêtre Quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.

3. Sous l'onglet **Quarantaine**, cliquez sur le bouton **Placer en quarantaine**.

4. Dans la fenêtre qui s'ouvre, choisissez le fichier qu'il faut placer en quarantaine.

Pour placer un fichier en quarantaine à l'aide du menu contextuel, procédez comme suit :

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier contenant le fichier à mettre en quarantaine.

2. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Copier dans la quarantaine**.

Pour analyser un fichier en quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.

3. Sous l'onglet **Quarantaine**, sélectionnez le fichier qu'il faut analyser.

4. Cliquez sur le bouton **Analyser**.

Pour restaurer un fichier depuis la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.

3. Sous l'onglet **Quarantaine**, sélectionnez le fichier qu'il faut restaurer.

4. Cliquez sur le bouton **Restaurer**.

Pour supprimer un fichier depuis la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.

3. Sous l'onglet **Quarantaine**, sélectionnez le fichier qu'il faut supprimer.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Supprimer**.

Pour envoyer l'objet en quarantaine à Kaspersky Lab pour étude, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.

3. Sous l'onglet **Quarantaine**, sélectionnez le fichier qu'il faut envoyer pour examen.

4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Envoyer pour étude**.

MANIPULATION D'OBJETS DANS LA SAUVEGARDE

La sauvegarde de Kaspersky Anti-Virus permet d'exécuter les opérations suivantes :

- Restaurer les fichiers dans un dossier désigné ou dans les dossiers d'origine où ils se trouvaient avant le traitement par Kaspersky Anti-Virus ;
- Supprimer les fichiers sélectionnés ou tous les fichiers dans la sauvegarde.

Pour restaurer un fichier depuis la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.
3. Sous l'onglet **Sauvegarde**, sélectionnez le fichier qu'il faut restaurer.
4. Cliquez sur le bouton **Restaurer**.

Pour supprimer un fichier depuis la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.
3. Sous l'onglet **Sauvegarde**, sélectionnez le fichier qu'il faut supprimer.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Supprimer**.

Pour supprimer tous les fichiers depuis la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.
3. Sous l'onglet **Sauvegarde**, cliquez sur le bouton **Purger le dossier de sauvegarde**.

ANALYSE DES FICHIERS EN QUARANTAINE APRES LA MISE A JOUR

Si l'analyse du fichier n'a pas permis de définir exactement la nature des programmes malveillants qui l'ont infecté, il est placé en quarantaine. Il se peut, après la mise à jour des bases, que Kaspersky Anti-Virus puisse identifier la menace et la supprimer. Vous pouvez activer l'analyse automatique des fichiers en quarantaine après chaque mise à jour.

Nous vous conseillons d'examiner fréquemment les fichiers en quarantaine. Leur statut peut changer après l'analyse. Certains fichiers pourront être restaurés dans leur emplacement d'origine et être à nouveau utilisés.

Pour activer l'analyse des objets en quarantaine après la mise à jour, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez dans la section **Mise à jour** le composant **Paramètres de la mise à jour**.
3. Dans le groupe **Avancé**, cochez la case **Analyser les fichiers en quarantaine après une mise à jour**.

OUTILS DE PROTECTION COMPLEMENTAIRE

Afin d'exécuter des tâches spécifiques à la protection de l'ordinateur, Kaspersky Anti-Virus propose une série d'Assistants et d'outils.

- L'Assistant Kaspersky Rescue Disk permet de créer une image de disque et d'enregistrer l'application Kaspersky Rescue Disk sur un support amovible afin de pouvoir remettre un système en état de marche après une attaque de virus grâce au démarrage depuis le support amovible. Kaspersky Rescue Disk intervient dans les cas d'infection qui rendent la réparation de l'ordinateur impossible à l'aide des logiciels antivirus ou des outils de réparation.

- L'Assistant de suppression des traces d'activité est prévu pour la recherche et la suppression des traces d'activité de l'utilisateur dans le système ainsi que des paramètres du système d'exploitation qui permettent d'accumuler des données sur l'activité de l'utilisateur.

- L'Assistant de restauration du système permet de supprimer les corruptions et les traces laissées par des objets malveillants dans le système.

- L'Assistant de Configuration du navigateur est prévu pour l'analyse et la configuration des paramètres de Microsoft Internet Explorer dans le but de supprimer les vulnérabilités potentielles.

Tous les problèmes découverts par les Assistants (sauf l'Assistant de création de Kaspersky Rescue Disk) sont regroupés en fonction du danger qu'ils représentent pour le système. Pour chaque groupe de problèmes, les experts de Kaspersky Lab proposent un ensemble d'actions dont l'exécution permettra de supprimer les vulnérabilités et les points problématiques du système. Il existe trois groupes de problèmes et par conséquent, trois groupes d'actions exécutées.

- *Les actions vivement recommandées* permettent de supprimer les problèmes qui constituent une menace sérieuse pour la sécurité. Il est conseillé d'exécuter dans les plus brefs délais toutes les actions de ce groupe pour supprimer la menace.

- *Les actions recommandées* visent à supprimer les problèmes qui peuvent présenter un danger potentiel. Il est également conseillé d'exécuter les actions de ce groupe pour garantir une protection optimale.

- *Les actions complémentaires* sont prévues pour supprimer les problèmes qui ne présentent actuellement aucun danger mais qui à l'avenir pourraient menacer la sécurité de l'ordinateur. L'exécution de ces actions garantit la protection totale de l'ordinateur mais peut, dans certains cas, entraîner la suppression de certains paramètres définis par l'utilisateur (par exemple, les cookies).

DANS CETTE SECTION

SUPPRESSION DES TRACES D'ACTIVITE

Lorsque vous utilisez votre ordinateur, vos activités sont enregistrées dans le système. Les données relatives aux recherches lancées par l'utilisateur et aux sites visités sont conservées, tout comme les données relatives à l'exécution d'applications et à l'ouverture et à l'enregistrement de fichiers, les entrées du journal système Microsoft Windows, les fichiers temporaires et bien d'autres encore.

Toutes ces sources d'informations sur l'activité de l'utilisateur peuvent contenir des données confidentielles (y compris des mots de passe) que les individus malintentionnés pourraient analyser. Bien souvent, l'utilisateur ne possède pas les connaissances suffisantes pour empêcher le vol d'informations depuis ces sources.

Kaspersky Anti-Virus propose un Assistant de suppression des traces d'activité. Cet Assistant recherche les traces d'activité de l'utilisateur dans le système ainsi que les paramètres du système d'exploitation qui permettent de récolter des informations sur cette activité.

Il ne faut pas oublier que des informations sur l'activité de l'utilisateur dans le système sont accumulées sans cesse. L'exécution du moindre fichier ou l'ouverture de n'importe quel document est enregistrée dans l'historique et le journal de Microsoft Windows enregistre une multitude d'événements qui surviennent dans le système. Ceci veut dire qu'une nouvelle exécution de l'Assistant de suppression des traces d'activité peut découvrir des traces supprimées lors de l'exécution antérieure de l'Assistant. Certains fichiers, par exemple le fichier de rapport de Microsoft Windows, peuvent être utilisés par le système au moment où les traces sont supprimées par l'Assistant. Afin de pouvoir supprimer ces fichiers, l'Assistant propose de redémarrer le système. Toutefois, ces fichiers peuvent être recréés lors du redémarrage, ce qui signifie qu'ils seront à nouveau découverts en tant que trace d'activité.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Pour supprimer les traces de l'activité de l'utilisateur dans le système, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils**.
3. Dans le groupe **Suppression des traces d'activité** de la fenêtre qui s'ouvre, cliquez sur le bouton **Exécuter**.

Examinons en détails les étapes de l'Assistant.

Etape 1. Début de l'utilisation de l'Assistant

Assurez-vous que l'option **Rechercher les Traces d'activité de l'utilisateur** a été sélectionnée, puis appuyez sur le bouton **Suivant** pour lancer l'Assistant.

Etape 2. Recherche de traces d'activité

L'Assistant recherche les traces d'activité sur votre ordinateur. La recherche peut durer un certain temps. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 3. Sélection des actions pour la suppression des traces d'activité

A la fin de la recherche, l'Assistant indique les traces d'activité trouvées et les moyens proposés pour s'en débarrasser.

Pour voir les actions reprises dans le groupe, cliquez sur le signe **+** situé à gauche du nom du groupe.

Pour que l'Assistant réalise une action, cochez la case à gauche du nom de l'action. Toutes les actions recommandées et vivement recommandées sont exécutées par défaut. Si vous ne souhaitez pas exécuter une action quelconque, désélectionnez la case en regard de celle-ci.

Il est vivement déconseillé de décocher les cases sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.

Une fois que vous aurez sélectionné les actions pour l'Assistant, cliquez sur **Suivant**.

Etape 4. Suppression des traces d'activité

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des traces d'activité peut durer un certain temps. La suppression de certaines traces d'activité nécessitera peut-être le redémarrage de l'ordinateur. L'Assistant vous préviendra.

Une fois les traces d'activité supprimée, l'Assistant passe automatiquement à l'étape suivante.

Etape 5. Fin de l'Assistant

Si vous souhaitez que la suppression des traces d'activité soit réalisée automatiquement à l'avenir au moment de quitter Kaspersky Anti-Virus, cochez la case **Supprimer les traces d'activité à chaque arrêt de Kaspersky Anti-Virus** à la dernière étape de l'Assistant. Si vous avez l'intention de supprimer vous-même les traces d'activité à l'aide de l'Assistant, sans cochez cette case.

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

CONFIGURATION DU NAVIGATEUR POUR LA NAVIGATION SECURISEE

Dans certains cas, le navigateur Microsoft Internet Explorer requiert une analyse et une configuration spéciales des paramètres car certaines valeurs, définies par les utilisateurs ou présentes par défaut peuvent entraîner des problèmes au niveau de la sécurité.

Voici quelques exemples d'objets et de paramètres utilisés par le navigateur et qui constituent une menace potentielle pour la sécurité.

- **Cache de fonctionnement de Microsoft Internet Explorer**. Le cache conserve les données téléchargées depuis Internet, ce qui permet de ne pas les télécharger de nouveaux par la suite. Ceci diminue le temps de téléchargement des pages web et diminue le trafic Internet. Par ailleurs, le cache contient les données confidentielles et offre la possibilité de connaître les ressources visitées par l'utilisateur. Nombreux sont les objets malveillants qui, lors du balayage du disque, balaient également le cache, ce qui signifie que les individus malintentionnés peuvent obtenir, par exemple, les adresses de messagerie des utilisateurs. Pour augmenter la protection, il est recommandé de purger le cache après la fin du fonctionnement du navigateur.

- **Affichage de l'extension pour les fichiers de format connu**. Pour faciliter la modification des noms des fichiers, il est possible de ne pas afficher leurs extensions. Cependant, il est utile par fois pour l'utilisateur de voir l'extension réelle du fichier. Les noms de fichier de nombreux objets malveillants utilisent des combinaisons de caractères qui imitent une extension supplémentaire avant l'extension réelle (par exemple, ceciestunexemple.txt.com). Si l'extension réelle du fichier n'est pas affichée, l'utilisateur voit uniquement la partie du fichier avec l'imitation de l'extension et peut considérer l'objet malveillant comme un objet ne présentant aucun danger. Pour augmenter la protection, il est recommandé d'activer l'affichage des extensions pour les fichiers de formats connus.

- **Liste des sites de confiance**. Pour le fonctionnement correct de certains sites web, il faut les ajouter dans la liste de confiance. Par ailleurs, les objets malveillants peuvent ajouter à cette liste les liens sur les sites web créés par les malfaiteurs.

La configuration du navigateur pour la navigation sécurisée peut entraîner des problèmes d'affichage pour certains sites (par exemple, s'ils utilisent des éléments ActiveX). Vous pouvez résoudre ce problème en ajoutant ces sites web à la zone de confiance.

L'analyse et la configuration du navigateur sont confiées à l'Assistant de configuration du navigateur. L'Assistant vérifie si les mises à jour les plus récentes du navigateur ont été installées et si les valeurs des paramètres définies ne rendent pas le système vulnérable aux actions des individus malintentionnés. Pour conclure, l'Assistant rédige un rapport qui peut être envoyé à Kaspersky Lab pour analyse.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Avant de lancer le diagnostic, fermez toutes les fenêtres de Microsoft Internet Explorer.

Pour configurer le navigateur pour la navigation sécurisée, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils**.
3. Dans le groupe **Configuration du navigateur** de la fenêtre qui s'ouvre, cliquez sur le bouton **Exécuter**.

Examinons en détails les étapes de l'Assistant.

Etape 1. Début de l'utilisation de l'Assistant

Assurez-vous que l'option **Analyser Microsoft Internet Explorer** a été sélectionnée, puis appuyez sur le bouton **Suivant** pour lancer l'Assistant.

Etape 2. Analyse de la configuration de Microsoft Internet Explorer

L'Assistant analyse les paramètres du navigateur Microsoft Internet Explorer. La recherche de problèmes dans les paramètres peut prendre un certain temps. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 3. Sélection des actions pour la configuration du navigateur

A la fin de la recherche, l'Assistant indique les problèmes détectés et les moyens proposés pour s'en débarrasser.

Pour voir les actions reprises dans le groupe, cliquez sur le signe **+** situé à gauche du nom du groupe.

Pour que l'Assistant réalise une action, cochez la case à gauche du nom de l'action. Toutes les actions recommandées et vivement recommandées sont exécutées par défaut. Si vous ne souhaitez pas exécuter une action quelconque, désélectionnez la case en regard de celle-ci.

Il est vivement déconseillé de décocher les cases sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.

Une fois que vous aurez sélectionné les actions pour l'Assistant, cliquez sur **Suivant**.

Etape 4. Configuration du navigateur

L'Assistant exécute les actions sélectionnées à l'étape précédente. La configuration du navigateur peut durer un certain temps. Une fois la configuration terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 5. Fin de l'Assistant

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

ANNULATION DES MODIFICATIONS INTRODUITES PAR LES ASSISTANTS

Il est possible d'annuler certaines modifications introduites par l'Assistant de suppression des traces d'activité (cf. section "Suppression des traces d'activité" à la page 118), l'Assistant de restauration du système (cf. section "Que faire si vous pensez que votre ordinateur est infecté" à la page 52), l'Assistant de configuration du navigateur (cf. section "Configuration du navigateur" à la page 120).

Pour annuler les modifications introduites par les Assistants, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Outils**.

2. Dans la partie droite de la fenêtre, cliquez sur le bouton **Exécuter** dans le groupe portant le nom de l'Assistant dont les modifications doivent être annulées :

   - **Suppression des traces d'activité** : pour annuler les modifications introduites par l'Assistant de suppression des traces d'activité ;

- **Restauration du système** : pour annuler les modifications introduites par l'Assistant de restauration du système ;
- **Configuration du navigateur** : pour annuler les modifications introduites par l'Assistant de configuration du navigateur.

Examinons en détail les étapes des Assistants pour l'annulation des modifications.

Etape 1. Début de l'utilisation de l'Assistant

Sélectionnez l'option **Annuler les modifications**, puis cliquez sur le bouton **Suivant**.

Etape 2. Recherche des modifications

L'Assistant recherche les modifications qu'il a introduites et qui peuvent être annulées. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

Etape 3. Sélection des modifications à annuler

A la fin de la recherche, l'Assistant signale les modifications détectées.

Pour qu'un Assistant annule les effets d'une action antérieure, cochez la case à gauche du nom de l'action.

Après avoir sélectionné les actions qu'il faut annuler, cliquez sur le bouton **Suivant**.

Etape 4. Annulation des modifications

L'Assistant annule les actions sélectionnées à l'étape précédente. Une fois les modifications annulées, l'Assistant passe automatiquement à l'étape suivante.

Etape 5. Fin de l'Assistant

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

RAPPORTS

Les événements survenus pendant le fonctionnement des composants de la protection ou lors de l'exécution des tâches de Kaspersky Anti-Virus sont consignés dans des rapports.

DANS CETTE SECTION

COMPOSITION DU RAPPORT POUR LE COMPOSANT SELECTIONNE DE LA PROTECTION

Vous pouvez obtenir un rapport détaillé sur les événements survenus pendant le fonctionnement de chaque composant de la protection ou de chaque tâche de Kaspersky Anti-Virus.

Pour le confort d'utilisation des rapports, vous pouvez gérer la représentation des données à l'écran : regrouper les événements selon divers paramètres, sélectionner la période couverte par le rapport, trier les événements dans chaque colonne ou selon l'importance et masquer des colonnes du tableau.

Pour obtenir un rapport pour le composant de la protection ou la tâche, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre **Rapports** qui s'ouvre, cliquez sur le bouton **Rapport détaillé**.
4. Dans la partie gauche de la fenêtre **Rapport détaillé** qui s'ouvre, sélectionnez le composant ou la tâche pour lequel vous souhaitez créer un rapport. Si vous sélectionnez l'option **Protection**, le rapport sera produit pour tous les composants de la protection.

FILTRAGE DES DONNEES

Les rapports de Kaspersky Anti-Virus permettent de filtrer les événements selon une ou plusieurs valeurs dans les colonnes du tableau, voire de définir des conditions de filtrage complexe.

Pour filtrer les événements selon des valeurs, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre **Rapports** qui s'ouvre, cliquez sur le bouton **Rapport détaillé**.
4. Dans la partie droite de la fenêtre **Rapport détaillé**, placez le curseur sur le coin supérieur gauche de l'en-tête de la colonne, puis ouvrez le menu du filtre en cliquant sur le bouton gauche de la souris.
5. Dans le menu du filtre, choisissez la valeur à utiliser pour filtrer les données.
6. Le cas échéant, répétez la procédure pour une autre colonne du tableau.

Pour définir des conditions de filtrage complexe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre afin d'ouvrir la fenêtre des rapports.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport**, cliquez sur le bouton **Rapport détaillé**.
4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la colonne du rapport requise, puis sélectionnez l'option **Filtre**.
5. Dans la fenêtre **Filtre complexe**, définissez les conditions nécessaires du filtrage.
   a. Dans la partie droite de la fenêtre, définissez la limite de la sélection.

b. Dans la partie gauche de la fenêtre, dans la liste déroulante **Condition**, choisissez la condition de sélection (par exemple, supérieure à ou inférieure à, égale à ou différente de la valeur indiquée en tant que limite de la sélection).

c. Le cas échéant, ajoutez une deuxième valeur à l'aide d'un opérateur logique de conjonction (ET) ou de disjonction (OU). Si vous souhaitez que la sélection des données vérifie les deux conditions définies, sélectionnez **ET**. Si une condition minimum suffit, sélectionnez **OU**.

RECHERCHE D'EVENEMENTS

Vous pouvez rechercher l'événement souhaité dans le rapport à l'aide d'un mot clé via la barre de recherche ou à l'aide d'une fenêtre de recherche spéciale.

Pour trouver un événement à l'aide de la barre de recherche, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre **Rapports** qui s'ouvre, cliquez sur le bouton **Rapport détaillé**.
4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, saisissez le mot clé dans la barre de recherche.

Pour trouver un événement à l'aide de la fenêtre de recherche, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre **Rapports** qui s'ouvre, cliquez sur le bouton **Rapport détaillé**.
4. Dans la partie droite de la fenêtre **Rapport détaillé** qui s'ouvre, cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la colonne du rapport requise, puis sélectionnez l'option **Recherche**.
5. Dans la fenêtre **Recherche** qui s'ouvre, définissez les critères de la recherche.

   a. Dans le champ **Ligne**, saisissez le mot clé pour la recherche.

   b. Dans la liste déroulante **Colonne**, sélectionnez le nom de la colonne dans laquelle il faudra rechercher le mot clé saisi.

   c. Le cas échéant, cochez les cases pour des paramètres de recherche complémentaires.
6. Lancez la recherche selon une des méthodes suivantes :

   - Si vous souhaitez chercher le prochain événement répondant aux critères de recherche définis après l'événement sélectionné dans la liste, cliquez sur **Recherche**.
   - Si vous souhaitez trouver tous les événements qui répondent aux critères de recherche définis, cliquez sur le bouton **Marquer tout**.

ENREGISTREMENT DU RAPPORT DANS UN FICHIER

Vous pouvez exporter le rapport obtenu dans un fichier texte.

Pour enregistrer le rapport dans un fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre.

3. Dans la fenêtre **Rapports** qui s'ouvre, cliquez sur le bouton **Rapport détaillé**.

4. Dans la fenêtre ouverte **Rapport détaillé**, formez le rapport requis et à l'aide du lien **Exporter** ouvrez la fenêtre pour sélectionner l'emplacement du fichier à enregistrer.

5. Dans la fenêtre qui s'ouvre, désignez le répertoire dans lequel il faut enregistrer le fichier du rapport et saisissez le nom du fichier.

CONSERVATION DES RAPPORTS

La durée maximale de conservation des rapports sur les événements est limitée à 30 jours. Les données sont supprimées à l'issue de cette période. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

De plus, vous pouvez également indiquer la taille maximale du fichier du rapport. Par défaut, la taille maximale est limitée à 1 024 Mo. Une fois que la taille maximale est atteinte, le contenu du fichier est remplacé par de nouveaux enregistrements. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

- *Pour configurer la durée maximale de conservation des rapports, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.

  2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Rapports et stockages**.

  3. Dans la partie droite de la fenêtre, dans le groupe **Conservation des rapports**, cochez la case **Supprimer les rapports après** et indiquez la durée maximale de la conservation des rapports.

- *Pour configurer la taille maximale du fichier de rapport, procédez comme suit :*

  1. Ouvrez la fenêtre de configuration de l'application.

  2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Rapports et stockages**.

  3. Dans la partie droite de la fenêtre, dans le groupe **Conservation des rapports**, cochez la case **Taille maximale de fichier** et indiquez la taille maximale du fichier de rapport.

PURGE DES RAPPORTS

Vous pouvez purger les rapports dont les données ne vous sont plus utiles.

- *Pour purger les rapports, procédez comme suit* :

  1. Ouvrez la fenêtre de configuration de l'application.

  2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Rapports et stockages**.

  3. Dans la partie droite de la fenêtre, dans le groupe **Purge des rapports**, cliquez sur **Purger**.

  4. Dans la fenêtre **Suppression des informations des rapports** qui s'ouvre, cochez les cases en regard des rapports que vous souhaitez purger.

ENREGISTREMENT DES EVENEMENTS NON CRITIQUES DANS LE RAPPORT

Par défaut, les entrées relatives aux événements non critiques, aux événements du registre ou aux événements du système de fichiers ne sont pas ajoutées au rapport. Vous pouvez intégrer les entrées relatives à ces événements dans le rapport.

Pour consigner les événements non critiques dans le rapport, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Rapports et stockages**.
3. Dans la partie droite de la fenêtre, cochez la case **Ajouter les enregistrements des événements non critiques**.

CONFIGURATION DE LA NOTIFICATION SUR LA DISPONIBILITE DU RAPPORT

Vous pouvez programmer la fréquence selon laquelle Kaspersky Anti-Virus vous rappellera la disponibilité des rapports.

Pour configurer la notification sur la disponibilité du rapport, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapports** dans la partie supérieure de la fenêtre.
3. Dans la fenêtre **Rapports** qui s'ouvre, cliquez sur le bouton  .
4. Dans la fenêtre **Notifications** qui s'ouvre, définissez les paramètres de la programmation.

APPARENCE DE L'APPLICATION. ADMINISTRATION DES ELEMENTS ACTIFS DE L'INTERFACE

Kaspersky Anti-Virus permet de configurer les paramètres d'affichage d'un texte sur l'écran d'accueil de Microsoft Windows et des éléments actifs de l'interface (icône de l'application dans la zone de notification, fenêtres de notification et info-bulles).

DANS CETTE SECTION

TRANSPARENCE DES FENETRES DE NOTIFICATIONS

Pour activer la transparence des fenêtres de notification, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Apparence**.
3. Dans le groupe **Icône dans la barre des tâches**, cochez la case **Utiliser la transparence des fenêtres de notifications**.

ANIMATION DE L'ICONE DE L'APPLICATION DANS LA ZONE DE NOTIFICATIONS

L'animation de l'icône de l'application dans la zone de notifications a lieu pendant l'exécution de la mise à jour ou de l'analyse.

L'animation de l'icône de l'application dans la zone de notification est activée par défaut.

Pour désactiver l'animation de l'icône de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Apparence**.
3. Dans le groupe **Icône de la barre des tâches**, décochez la case **Animer l'icône durant l'exécution des tâches**.

TEXTE SUR L'ECRAN D'ACCUEIL DE MICROSOFT WINDOWS

Si Kaspersky Anti-Virus est activé et protège votre ordinateur, le texte "Protected by Kaspersky Lab" s'affiche par défaut sur l'écran d'accueil au démarrage de Microsoft Windows.

Le texte "Protected by Kaspersky Lab" s'affiche uniquement dans le système d'exploitation Microsoft Windows XP.

Pour désactiver l'affichage du texte au lancement de Microsoft Windows, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Apparence**.
3. Dans le groupe **Icône de la barre des tâches**, décochez la case **Afficher "Protected by Kaspersky Lab" sur l'écran de bienvenue de Microsoft Windows**.

NOTIFICATIONS

Par défaut, lorsqu'un événement se produit pendant l'utilisation de Kaspersky Anti-Virus vous prévient. Si vous devez exécuter une action quelconque, une fenêtre de notification apparaît (cf. section "Fenêtre de notification et messages contextuels" à la page 34). Les événements qui ne requièrent pas la sélection d'une action sont signalés à l'aide d'une notification sonore, de messages électronique ou de messages contextuels dans la zone de notification de la barre des tâches (cf. section "Fenêtre de notification et messages contextuels" à la page 34).

Kaspersky Anti-Virus inclut le kiosque d'informations (cf. page 37) à l'aide duquel Kaspersky Lab vous notifie sur les informations. Si vous voulez recevoir des informations, vous pouvez activer l'envoi des informations.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DES NOTIFICATIONS

Par défaut Kaspersky Anti-Virus vous signale les événements importants liés au fonctionnement de l'application de différentes manières (cf. section "Configuration des modes de notification" à la page 128). Vous pouvez désactiver l'affichage des notifications.

Que la remise des notifications soit activée ou non, les informations relatives aux événements survenus pendant le fonctionnement de Kaspersky Anti-Virus sont consignées dans le rapport sur le fonctionnement de l'application (cf. page 122).

La désactivation de la remise des notifications n'a aucune influence sur l'affichage des fenêtres de notification. Pour réduire au minimum l'affichage de fenêtre de notification, utilisez le mode de protection automatique (cf. section "Sélection du mode de protection" à la page 64).

Pour désactiver la remise des notifications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Notifications**.
3. Dans la partie droite de la fenêtre, décochez la case **Activer les notifications**.

CONFIGURATION DES MODES DE NOTIFICATION

L'application vous signale les événements d'une des méthodes suivantes :

- message contextuel dans la zone de notification de la barre des tâches ;
- notification sonore ;
- messages électroniques.

Vous pouvez configurer les modes de notification pour chaque type d'événement.

Par défaut, les notifications critiques et les notifications sur les violations du fonctionnement de l'application sont accompagnées d'une notification sonore. Les notifications sonores utilisent la gamme de sons de Microsoft Windows. Vous pouvez changer la gamme de sons ou désactiver la notification sonore.

Pour que Kaspersky Anti-Virus puisse vous signaler les événements par courrier électronique, il faut configurer les paramètres du courrier électronique pour la remise des notifications.

Pour configurer les modes de notification pour différents types d'événements, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Notifications**.
3. Dans la partie droite de la fenêtre, cochez la case **Activer les notifications**, puis cliquez sur **Configuration**, sous la case.
4. Dans la fenêtre **Notifications** qui s'ouvre, cochez les cases en fonction des modes de notification que vous voulez utiliser pour les divers événements : par courrier électronique, dans un message contextuel ou via une notification sonore.

Pour configurer les paramètres du courrier électronique pour l'envoi des notifications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Notifications**.
3. Dans la partie droite de la fenêtre, cochez la case **Activer les notifications par courriers**, puis cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Configuration des notifications par courrier** qui s'ouvre, définissez les paramètres de remise des notifications par courrier électronique.

Pour modifier la gamme de sons des notifications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Notifications**.
3. Dans la partie droite de la fenêtre, cochez la case **Activer les sons**.

   Si vous souhaitez utiliser les sons de Microsoft Windows pour les notifications relatives aux événements de Kaspersky Lab, cochez la case **Utiliser les sons standards de Windows par défaut**. Si la case est décochée, c'est la sélection de sons des versions antérieures de Kaspersky Anti-Virus qui sera utilisée.

DESACTIVATION DE LA REMISE DES INFOS

Pour désactiver la réception des informations depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, dans la section **Paramètres avancés**, sélectionnez la sous-section **Apparence**.
3. Dans la partie droite de la fenêtre, décochez la case **M'avertir des informations de Kaspersky Lab**.

KASPERSKY SECURITY NETWORK

Afin d'améliorer l'efficacité de la protection de votre ordinateur, Kaspersky Anti-Virus utilise les données obtenues auprès d'utilisateurs issus du monde entier. Le réseau Kaspersky Security Network permet de récolter ces données.

Kaspersky Security Network (KSN) est un ensemble de services en ligne qui permet d'accéder à la base de connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. L'utilisation des données

de Kaspersky Security Network permet à l'application de réagir plus rapidement aux nouvelles formes de menace, améliore l'efficacité de certains composants de la protection et réduit la probabilité de faux positifs.

L'implication des utilisateurs dans le Kaspersky Security Network permet à Kaspersky Lab de recueillir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des moyens de neutralisation et de réduire le nombre de faux positifs.

De plus, la participation au Kaspersky Security Network vous donne accès aux données sur la réputation des applications et des sites Web.

La participation au Kaspersky Security Network signifie que certaines statistiques obtenues pendant l'utilisation de Kaspersky Anti-Virus sur votre ordinateur sont envoyées automatiquement à Kaspersky Lab.

Vos données personnelles ne sont ni recueillies, ni traitées, ni enregistrées.

La participation au Kaspersky Security Network est volontaire. Vous prenez cette décision pendant l'installation de Kaspersky Anti-Virus, mais vous pouvez la changer à tout moment.

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DE LA PARTICIPATION A KASPERSKY SECURITY NETWORK

Pour participer au Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, choisissez la sous-section **Retour d'informations** dans la section **Paramètres avancés**.
3. Dans la partie droite de la fenêtre, cochez la case **J'accepte de rejoindre le Kaspersky Security Network**.

VERIFICATION DE CONNEXION A KASPERSKY SECURITY NETWORK

La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :

- Votre ordinateur n'est pas connecté à Internet ;
- Vous ne participez pas au Kaspersky Security Network ;
- Votre licence d'utilisation de Kaspersky Anti-Virus est limitée.

Pour vérifier la connexion à Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton **Cloud Protection** dans la partie supérieure de la fenêtre.
3. La partie gauche de la fenêtre ouverte affiche l'état de la connexion à Kaspersky Security Network.

VERIFICATION DU FONCTIONNEMENT DE L'APPLICATION

Cette section explique comment vérifier le fonctionnement de l'application : confirmer la détection des virus et de leurs modifications ainsi que l'exécution de l'action requise sur ces derniers.

DANS CETTE SECTION

PRESENTATION DU FICHIER D'ESSAI EICAR

Vous pouvez utiliser un *fichier d'essai EICAR* pour confirmer que l'application est capable de détecter des virus et de réparer les fichiers infectés. Le fichier d'essai EICAR a été développé par l'European Institute for Computer Antivirus Research (EICAR) afin d'analyser le fonctionnement des logiciels antivirus.

Le fichier d'essai EICAR n'est pas un virus. Le fichier d'essai EICAR ne contient aucun code informatique capable de nuire à l'ordinateur. Mais la majorité des logiciels antivirus identifie le fichier d'essai EICAR en tant que virus.

Le fichier d'essai EICAR n'est pas prévu pour tester le fonctionnement de l'analyse heuristique ou la recherche de programmes malveillants au niveau du système (outils de dissimulation d'activité).

N'utilisez en aucun cas de véritables virus afin de tester le fonctionnement des logiciels antivirus ! Cela pourrait nuire à votre ordinateur.

N'oubliez pas de rétablir la protection antivirus du trafic Internet et des fichiers après avoir utilisé le fichier d'essai EICAR.

VERIFICATION DU FONCTIONNEMENT DE L'APPLICATION A L'AIDE DU FICHIER D'ESSAI EICAR

Vous pouvez vérifier l'efficacité de la protection du trafic Internet, de la protection antivirus des fichiers et de l'analyse de l'ordinateur à l'aide du fichier d'essai EICAR.

N'oubliez pas de rétablir la protection antivirus du trafic Internet et des fichiers après avoir utilisé le fichier d'essai EICAR.

Pour vérifier la protection du trafic Internet à l'aide du fichier d'essai EICAR, procédez comme suit :

1. Téléchargez le fichier d'essai EICAR depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

2. Essayez d'enregistrer le fichier d'essai EICAR dans n'importe quel dossier de votre ordinateur.

   Kaspersky Anti-Virus signale la détection d'une menace sur l'URL sollicitée et bloque l'enregistrement de l'objet sur l'ordinateur.

3. Le cas échéant, essayez les types du fichier d'essai EICAR (cf. section "Présentation des types du fichier d'essai EICAR" à la page 133).

Pour vérifier le fonctionnement de la protection antivirus des fichiers à l'aide du fichier d'essai EICAR ou de son type, procédez comme suit :

1. Suspendez la protection antivirus du trafic Internet et des fichiers sur votre ordinateur.

   Quand la protection est suspendue, il est déconseillé de connecter l'ordinateur au réseau local ou d'utiliser des disques amovibles afin d'éviter l'infection de l'ordinateur par des programmes malveillants.

2. Téléchargez le fichier d'essai EICAR depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

3. Enregistrez le fichier d'essai EICAR dans n'importe quel dossier de votre ordinateur.

4. Dans l'en-tête de la ligne du fichier d'essai EICAR ajoutez un des préfixes (cf. section "Présentation des types du fichier d'essai EICAR" à la page 133).

   Vous pouvez utiliser pour ce faire n'importe quel éditeur de texte ou d'hypertexte, par exemple le Bloc-notes. Pour lancer le Bloc-notes, sélectionnez **Démarrer** → **Applications** → **Standard** → **Bloc-notes**.

5. Enregistrez le fichier obtenu sous un nom correspondant au type du fichier EICAR : par exemple, si vous avez ajouté le préfixe DELE-, enregistrez le fichier obtenu sous le nom eicar_dele.com.

6. Rétablissez la protection antivirus du trafic Internet et des fichiers sur votre ordinateur.

7. Essayez de lancer le fichier enregistré.

   Kaspersky Anti-Virus vous signale la détection de menaces sur le disque dur de l'ordinateur et exécute l'action définie dans les paramètres de la protection antivirus des fichiers.

Pour vérifier le fonctionnement de la recherche de virus à l'aide du fichier d'essai EICAR ou de son type, procédez comme suit :

1. Suspendez la protection antivirus du trafic Internet et des fichiers sur votre ordinateur.

   Quand la protection est suspendue, il est déconseillé de connecter l'ordinateur au réseau local ou d'utiliser des disques amovibles afin d'éviter l'infection de l'ordinateur par des programmes malveillants.

2. Téléchargez le fichier d'essai EICAR depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

3. Dans l'en-tête de la ligne du fichier d'essai EICAR ajoutez un des préfixes (cf. section "Présentation des types du fichier d'essai EICAR" à la page 133).

   Vous pouvez utiliser pour ce faire n'importe quel éditeur de texte ou d'hypertexte, par exemple le Bloc-notes. Pour lancer le Bloc-notes, sélectionnez **Démarrer** → **Applications** → **Standard** → **Bloc-notes**.

4. Enregistrez le fichier obtenu sous un nom correspondant au type du fichier d'essai EICAR : par exemple, si vous avez ajouté le préfixe DELE-, enregistrez le fichier obtenu sous le nom eicar_dele.com.

5. Lancez l'analyse du fichier enregistré.

   Kaspersky Anti-Virus vous signale la détection de menaces sur le disque dur de l'ordinateur et exécute l'action définie dans les paramètres de l'analyse de l'ordinateur.

6. Rétablissez la protection antivirus du trafic Internet et des fichiers sur votre ordinateur.

PRESENTATION DES TYPES DU FICHIER D'ESSAI EICAR

Vous pouvez vérifier les fonctions de l'application en créant divers types du fichier d'essai EICAR. L'application détecte le fichier d'essai EICAR (son type) et lui attribue un statut en fonction des résultats de l'analyse. L'application exécute sur le fichier d'essai EICAR les actions configurées dans les paramètres du composant qui a détecté le fichier d'essai EICAR.

La première colonne du tableau (cf. tableau ci-après) contient les préfixes que vous pouvez utiliser pour créer des types du fichier d'essai EICAR. La deuxième colonne reprend toutes les valeurs possibles de l'état attribué au fichier par application à la fin de l'analyse. La troisième colonne contient les informations relatives au traitement que réservera l'application aux fichiers de l'état indiqué.

Tableau 2. Types du fichier d'essai EICAR

Préfixe	Etat du fichier	Informations sur le traitement du fichier
Pas de préfixe, virus d'essai standard.	**Infecté**. Le fichier contient le code d'un virus connu. La réparation du fichier est impossible.	L'application identifie ce fichier comme un fichier contenant un virus qui ne peut être réparé. La tentative de réparation du fichier s'opère selon l'action définie pour les fichiers infectés. Par défaut, l'application affiche un message qui indique que la réparation du fichier infecté est impossible.
CURE-	**Infecté**. Le fichier contient le code d'un virus connu. La réparation du fichier est possible.	Le fichier contient un virus qui peut être réparé ou supprimé. L'application répare le fichier et le texte du corps du virus est remplacé par CURE. L'application affiche un message qui signale la découverte d'un fichier infecté.
DELE-	**Infecté**. Le fichier contient le code d'un virus connu. La réparation du fichier est impossible.	L'application identifie ce fichier comme un virus qui ne peut être réparé et le supprime. L'application affiche un message qui signale la suppression d'un fichier infecté.
WARN-	**Potentiellement infecté**. Le fichier contient le code d'un virus inconnu. La réparation du fichier est impossible.	Le fichier est considéré comme potentiellement infecté. L'application exécute l'action définie pour les fichiers potentiellement infectés. Par défaut, l'application affiche une notification sur la détection d'un fichier potentiellement infecté.
SUSP-	**Potentiellement infecté.** Le fichier contient le code modifié d'un virus connu. La réparation du fichier est impossible.	L'application a découvert une équivalence partielle entre un extrait du code du fichier et un extrait du code d'un virus connu. Au moment de cette découverte du fichier potentiellement infecté, les bases de l'application ne contenaient pas la description du code complet de ce virus. L'application exécute l'action définie pour les fichiers potentiellement infectés. Par défaut, l'application affiche une notification sur la détection d'un fichier potentiellement infecté.
CORR-	**Corrompu**.	L'application n'analyse pas le fichier de ce type car sa structure est endommagée (par exemple, format de fichier non correct). Les informations relatives au traitement du fichier figurent dans le rapport sur le fonctionnement de l'application.
ERRO-	**Erreur d'analyse**.	Une erreur s'est produite lors de l'analyse du fichier. L'application ne peut accéder au fichier car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers le fichier (lorsque le fichier se trouve sur une ressource de réseau). Les informations relatives au traitement du fichier figurent dans le rapport sur le fonctionnement de l'application.

CONTACTER LE SUPPORT TECHNIQUE

Cette section présente les différentes méthodes d'obtention de l'assistance technique et les conditions à remplir pour pouvoir bénéficier de l'aide du service d'assistance technique.

DANS CETTE SECTION

MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous n'avez pas trouvé comment résoudre votre problème dans la documentation de l'application ou dans une des sources d'informations sur l'application (cf. section "Sources d'informations sur l'application" à la page 12), veuillez contacter le Support technique de Kaspersky Lab. Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application. Si l'ordinateur est infecté, les experts du service d'assistance technique essayeront de vous aider à supprimer les conséquences de l'exécution des programmes malveillants.

Avant de contacter le service d'assistance technique, veuillez lire les règles d'octroi de l'assistance technique à l'adresse Internet suivante : http://support.kaspersky.com/fr/support/consumer/tips.

Vous pouvez contacter les experts du service d'assistance technique d'une des manières suivantes :

- Via téléphone. Vous pouvez contacter les experts du service d'assistance technique en France.
- Via une demande depuis Mon Espace Personnel sur le site Web du service d'assistance technique. Cette méthode permet de contacter les experts du service d'assistance technique via un formulaire.

Afin de pouvoir obtenir l'assistance technique, vous devez être un utilisateur enregistré de la version commerciale de Kaspersky Anti-Virus. Les utilisateurs des versions d'évaluation n'ont pas accès à l'assistance technique.

Pour plus de détails, consultez sur notre site Internet : http://support.kaspersky.com/fr/support/consumer/tips.

UTILISATION DU FICHIER DE TRAÇAGE ET DU SCRIPT AVZ

Après avoir signalé le problème aux experts du service d'assistance technique, ceux-ci peuvent vous demander de composer un rapport reprenant les informations relatives au système d'exploitation et de l'envoyer au service d'assistance technique. Les experts du service d'assistance technique peuvent vous demander également de créer un *fichier de traçage*. Le fichier de traçage permet de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

L'analyse des données que vous envoyez permet aux experts du service d'assistance technique de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet d'analyser les processus exécutés à la recherche de code malveillant, de rechercher la présence de code malveillant dans le système, de réparer ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse du système.

CREATION D'UN RAPPORT SUR L'ETAT DU SYSTEME

Pour créer un rapport sur l'état du système, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Informations pour le service d'assistance technique**, cliquez sur le bouton **Créer le rapport sur l'état du système**.

Le rapport sur l'état du système est généré au format HTML et XML et il est enregistré dans l'archive sysinfo.zip. Une fois que la collecte des informations sur le système est terminée, vous pouvez consulter le rapport.

Pour consulter le rapport, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Informations pour le service d'assistance technique**, cliquez sur le bouton **Voir**.
4. Ouvrez l'archive sysinfo.zip contenant le fichier du rapport.

CREATION D'UN FICHIER DE TRACE

Afin de créer le fichier de trace, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Traçages** sélectionnez le niveau du traçage dans la liste déroulante.

   Il est recommandé de demander au spécialiste du Support technique le niveau du traçage requis. Faute d'indication du Support technique, il est conseillé d'établir le niveau du traçage à **500**.
4. Afin de lancer le traçage, cliquez sur le bouton **Activer**.
5. Reproduisez la situation où le problème apparaît.
6. Pour arrêter le traçage, cliquez sur le bouton **Désactiver**.

Vous pouvez passer au transfert des résultats du traçage (cf. section "Envoi des fichiers de données" à la page 135) sur le serveur de Kaspersky Lab.

ENVOI DES RAPPORTS

Une fois que les fichiers de traçage et le rapport sur l'état du système ont été créés, il faut les envoyer aux experts du Support technique de Kaspersky Lab.

Pour charger les fichiers de données sur le serveur du Support technique, il faut obtenir un numéro de requête. Ce numéro est accessible dans Mon Espace Personnel sur le site web du Support technique lorsque des requêtes actives sont présentes.

Pour télécharger les fichiers de données sur le serveur du Support technique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Actions**, cliquez sur le bouton **Envoyer les informations au service d'assistance technique**.

   La fenêtre **Chargement des informations pour l'assistance sur le serveur** s'ouvre.
4. Cochez les cases en regard des fichiers que vous souhaitez envoyer au Support technique, puis cliquez sur **Envoyer**.

   La fenêtre **Numéro de requête** s'ouvre.
5. Indiquez le numéro attribué à votre demande lors de l'appel au Support technique via Mon Espace Personnel et cliquez sur le bouton **OK**.

Les fichiers de données sélectionnés seront compactés et envoyés sur le serveur du Support technique.

S'il n'est pas possible pour une raison quelconque de contacter le Support technique, vous pouvez enregistrer les fichiers de données sur votre ordinateur et les envoyer plus tard depuis Mon Espace Personnel.

Pour enregistrer les fichiers de données sur le disque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, dans le groupe **Actions**, cliquez sur le bouton **Envoyer les informations au service d'assistance technique**.

   La fenêtre **Chargement des informations pour l'assistance sur le serveur** s'ouvre.
4. Cochez les cases en regard des fichiers que vous souhaitez envoyer au Support technique, puis cliquez sur **Envoyer**.

   La fenêtre **Numéro de requête** s'ouvre.
5. Cliquez sur le bouton **Annuler**, et dans la fenêtre qui s'ouvre confirmez l'enregistrement des fichiers sur le disque, en cliquant sur le bouton **Oui**.

   La fenêtre d'enregistrement des archives s'ouvre.
6. Saisissez le nom de l'archive et confirmez l'enregistrement.

Vous pouvez envoyer l'archive créée au Support technique via Mon Espace Personnel.

EXECUTION DU SCRIPT AVZ

Il est déconseillé de modifier le texte du script envoyé par les experts de Kaspersky Lab. En cas de problème lors de l'exécution du script, contactez le Support technique (cf. section "Modes d'obtention de l'assistance technique" à la page 134).

Pour exécuter le script AVZ, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Assistance technique** dans la partie inférieure de la fenêtre principale pour ouvrir la fenêtre **Assistance technique** dans laquelle vous cliquerez sur le lien **Outils d'assistance**.
3. Dans la fenêtre **Traçages** qui s'ouvre, cliquez sur le bouton **Exécuter le script AVZ**.

Si l'exécution du script réussi, l'Assistant termine. Si un échec se produit durant l'exécution du script, l'Assistant affiche le message correspondant.

ASSISTANCE TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du service d'assistance Français (http://www.kaspersky.com/fr/support).

Pour plus de renseignements, consultez sur notre site Internet : http://support.kaspersky.com/fr/support/consumer/tips.

OBTENTION DE L'ASSISTANCE TECHNIQUE VIA MON ESPACE PERSONNEL

Mon Espace Personnel est un espace qui vous est réservé https://my.kaspersky.com/fr sur le site du Support technique.

Pour pouvoir accéder à Mon Espace Personnel, vous devez vous inscrire sur la page d'enregistrement (https://my.kaspersky.com/fr/registration). Vous devrez saisir votre adresse de messagerie et un mot de passe d'accès à Mon Espace Personnel.

Mon Espace Personnel permet de réaliser les opérations suivantes :

- Envoyer des demandes au support technique et au laboratoire d'étude des virus ;
- Communiquer avec le support technique ;
- Obtenir une copie du fichier de licence en cas de perte ou de suppression de celui-ci.

Demande adressée par voie électronique au service d'assistance technique

Vous pouvez envoyer une demande par voie électronique au service d'assistance technique en anglais et en français.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- Type de demande ;
- Nom et numéro de version de l'application ;
- Texte de la demande ;
- Numéro de client et mot de passe ;
- Adresse de messagerie.

L'expert du service d'assistance technique répond via Mon Espace Personnel et en envoyant un message électronique à l'adresse indiquée dans la demande.

Demande électronique adressée au laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au service d'assistance technique mais au laboratoire d'étude des virus.

Vous pouvez envoyer les types de demandes suivantes au laboratoire d'étude des virus :

- *Programme malveillant inconnu* : vous soupçonnez le fichier de contenir un virus mais Kaspersky Anti-Virus ne détecte aucune infection.

  Les experts du laboratoire d'étude des virus analysent le code malveillant envoyé et en cas de découverte d'un virus inconnu jusque-là, ils ajoutent sa définition à la base des données accessible lors de la mise à jour des logiciels antivirus.

- *Faux positif du logiciel antivirus* : Kaspersky Anti-Virus considère un certain fichier comme un virus mais vous êtes convaincu que ce n'est pas le cas.

- *Demande de description d'un programme malveillant* : vous souhaitez obtenir la description d'un virus découvert par Kaspersky Anti-Virus sur la base du nom de ce virus.

Vous pouvez également envoyer une demande au laboratoire d'étude des virus depuis le formulaire de demande (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr), sans vous enregistrer dans Mon Espace Personnel. Dans ce cas, vous ne devez pas indiquer le code d'activation de l'application.

ANNEXES

Cette section contient des renseignements qui viennent compléter le contenu principal du document.

DANS CETTE SECTION

UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Anti-Virus à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- Activation de l'application ;
- Lancement et arrêt de l'application ;
- Lancement et arrêt des composants de l'application ;
- Lancement et arrêt des tâches ;
- Obtention d'informations relatives à l'état actuel des composants et aux tâches et à leur statistiques ;
- Lancement et arrêt de l'exécution des tâches d'analyse antivirus ;
- Analyse des objets sélectionnés ;
- Mise à jour des bases et des modules de l'application, retour à l'état antérieur à la mise à jour ;
- Exportation et importation des paramètres de la protection ;
- Affichage de l'aide sur la syntaxe de la ligne de commande pour l'ensemble des instructions ou pour des instructions individuelles.

Syntaxe de la ligne de commande :

```
avp.com <instruction> [paramètres]
```

La requête adressée à l'application via la ligne de commande doit être réalisée depuis le répertoire d'installation du logiciel ou en indiquant le chemin d'accès complet à avp.com.

La liste des instructions utilisées pour l'administration de l'application et de ses composants est reprise dans le tableau ci-dessous.

START	Lancement du composant ou de la tâche.
STOP	Arrêt du composant ou de la tâche (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Anti-Virus).
STATUS	Affichage de l'état actuel du composant ou de la tâche.

STATISTICS	Affichage des statistiques du composant ou de la tâche.
HELP	Affichage de la liste des instructions et des informations sur la syntaxe de l'instruction.
SCAN	Recherche d'éventuels virus dans les objets.
UPDATE	Lancement de la mise à jour de l'application.
ROLLBACK	Annulation de la dernière mise à jour réalisée (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Anti-Virus).
EXIT	Arrêt du logiciel (l'exécution de l'instruction est possible uniquement avec la saisie du mode passe défini via l'interface de l'application).
IMPORT	Importation des paramètres de protection de Kaspersky Anti-Virus (l'exécution de l'instruction est possible uniquement après saisie du mot de passe défini via l'interface de l'application).
EXPORT	Exportation des paramètres de la protection de l'application.

Chaque instruction possède ses propres paramètres, propres à chaque composant de l'application.

DANS CETTE SECTION

ACTIVATION DE L'APPLICATION

Kaspersky Anti-Virus peut être activé à l'aide du fichier de licence.

Syntaxe de l'instruction :

```
avp.com ADDKEY <nom_du_fichier>
```

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

<nom_du_fichier>	Nom du fichier de licence avec l'extension .key.

Exemple :

```
avp.com ADDKEY 1AA111A1.key
```

LANCEMENT DE L'APPLICATION

Syntaxe de l'instruction :

```
avp.com
```

ARRET DE L'APPLICATION

Syntaxe de l'instruction :

```
avp.com EXIT /password=<votre_mot_de_passe>
```

La description des paramètres est reprise dans le tableau ci-dessous.

<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface.

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

ADMINISTRATION DES COMPOSANTS DE L'APPLICATION ET DES TACHES

Syntaxe de l'instruction :

```
avp.com <instruction> <profil|nom_de_la_tâche> [/R[A]:<fichier_de_rapport>]
avp.com STOP <profil|nom_de_la_tâche> /password=<votre_mot_de_passe>
[/R[A]:<fichier_de_rapport>]
```

Les instructions et les paramètres sont décrits dans le tableau ci-après.

<instruction>	L'administration des composants et des tâches de Kaspersky Anti-Virus via la ligne de commande s'opère à l'aide des instructions suivantes : START : lancement du composant de la protection en temps réel ou d'une tâche. STOP : arrêt du composant de la protection en temps réel ou d'une tâche. STATUS : affichage de l'état actuel du composant de la protection ou d'une tâche. STATISTICS : affichage des statistiques du composant de la protection ou d'une tâche. N'oubliez pas que l'instruction STOP ne peut être exécutée sans la saisie préalable du mot de passe.
<profil|nom_de_la_tâche>	En guise de valeur pour le paramètre **<profil>**, vous pouvez indiquer n'importe quel composant de la protection de Kaspersky Anti-Virus ainsi que les modules qui sont repris dans les composants des tâches d'analyse à la demande ou de mise à jour composées (les valeurs standard utilisées par l'application sont reprises dans le tableau ci-après). En guise de valeur pour le paramètre **<nom_de_la_tâche>**, vous pouvez indiquer le nom de n'importe quelle tâche d'analyse à la demande ou de mise à jour configurée par l'utilisateur.
<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface.

/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants. **/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

Le paramètre **<profil>** prend une des valeurs du tableau ci-après.

RTP	Tous les composants de la protection. L'instruction **avp.com START RTP** lance tous les composants de la protection, si la protection avait été arrêtée. Si le composant a été arrêté via l'instruction **STOP** de la ligne de commande, il ne pourra être redémarré via l'instruction **avp.com START RTP**. Pour ce faire, il faut exécuter l'instruction **avp.com START <profil>** où le paramètre **<profil>** représente un composant concret de la protection, par exemple **avp.com START FM**.
pdm	Défense Proactive.
FM	Antivirus Fichiers.
EM	Antivirus Courrier.
WM	Antivirus Internet. Valeurs pour les sous-composants de l'Antivirus Internet : **httpscan (HTTP)** : analyse du trafic HTTP ; **sc** : analyse des scripts.
IM	Antivirus IM ("Chat").
Updater	Mise à jour.
Rollback	Annulation de la dernière mise à jour.
Scan_My_Computer	Analyse de l'ordinateur.
Scan_Objects	Analyse des objets.
Scan_Quarantine	Analyse de la quarantaine.
Scan_Startup (STARTUP)	Analyse des objets de démarrage.
Scan_Vulnerabilities (SECURITY)	Recherche de vulnérabilités.

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

Exemples :

- *Pour activer l'Antivirus Fichiers, saisissez l'instruction :*

```
avp.com START FM
```

- *Pour arrêter l'analyse de l'ordinateur, saisissez l'instruction :*

```
avp.com STOP Scan_My_Computer /password=<votre_mot_de_passe>
```

RECHERCHE DE VIRUS

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour lancer le traitement des objets malveillants découverts ressemble à ceci :

```
avp.com SCAN [<objet à analyser>] [<action>] [<types de fichiers>] [<exclusions>]
[<fichier de configuration>] [<paramètres du rapport>] [< paramètres complémentaires
>]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans l'application en lançant la tâche requise via la ligne de commande. Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface de Kaspersky Anti-Virus.

La description des paramètres est reprise dans le tableau ci-dessous.

<objet à analyser> : ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
<files>	Liste des chemins d'accès aux fichiers et aux répertoires à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarques : • Mettre le nom de l'objet entre guillemets s'il contient un espace ; • Lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/MEMORY	Objets de la mémoire vive.
/STARTUP	Objets de démarrage.
/MAIL	Boîtes aux lettres.
/REMDRIVES	Tous les disques amovibles.
/FIXDRIVES	Tous les disques locaux.
/NETDRIVES	Tous les disques de réseau.
/QUARANTINE	Objets en quarantaine.
/ALL	Analyse complète de l'ordinateur.
/@:<filelist.lst>	Chemin d'accès au fichier de la liste des objets et répertoires inclus dans l'analyse. La saisie d'un chemin d'accès relatif ou absolu au fichier est autorisée. Le chemin doit être saisi sans guillemets, même s'il contient un espace. Le fichier contenant la liste des objets doit être au format texte. Chaque objet à analyser doit se trouver sur une nouvelle ligne. Il est conseillé de saisir dans le fichier les chemins d'accès absolu aux objets à analyser. Si un chemin d'accès relatif est saisi, le chemin est indiqué par rapport au fichier exécutable de l'application et non pas par rapport au fichier contenant la liste des objets à analyser.

<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur **/i8**. Si vous travaillez en mode automatique, alors Kaspersky Anti-Virus appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. L'action définie par la valeur du paramètre **<action>** sera ignorée.	
/i0	Aucune action n'est exécutée, les informations sont consignées dans le rapport.
/i1	Réparer les objets infectés, si la réparation est impossible, les ignorer.
/i2	Réparer les objets infectés, si la réparation est impossible, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive sfx).
/i3	Réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i4	Supprimer les objets infectés ; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i8	Confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté.
/i9	Confirmer l'action auprès de l'utilisateur à la fin de l'analyse.
Le paramètre **<types de fichiers>** définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu.	
/fe	Analyser uniquement les fichiers qui peuvent être infectés selon l'extension.
/fi	Analyser uniquement les fichiers qui peuvent être infectés selon le contenu.
/fa	Analyser tous les fichiers.
Le paramètre **<exclusions>** définit les objets exclus de l'analyse. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
-e:a	Ne pas analyser les archives.
-e:b	Ne pas analyser les bases de messagerie.
-e:m	Ne pas analyser les messages électroniques au format plain text.
-e:<filemask>	Ne pas analyser les objets en fonction d'un masque.
-e:<secondes>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre **<secondes>**.
-es:<taille>	Ignorer les objets dont la taille (en Mo) est supérieure à la valeur définie par le paramètre **<taille>**. Le paramètre s'applique uniquement aux fichiers composés (par exemple, aux archives).
Le **<fichier de configuration>** définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par l'application pour l'analyse. Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour l'analyse antivirus. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.	
/C:<nom_du_fichier>	Utiliser les valeurs des paramètres définies dans le fichier de configuration **<nom_du_fichier>**.

Le **<paramètres du rapport>** définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.	
/R:<fichier_de_rapport>	Consigner uniquement les événements importants dans le fichier indiqué.
/RA:<fichier_de_rapport>	Consigner tous les événements dans le fichier de rapport indiqué.
<paramètres complémentaires> : paramètres qui définissent l'utilisation de technologies de recherche de virus.	
/iChecker=<on|off>	Active/désactive l'utilisation de la technologie iChecker.
/iSwift=<on|off>	Active/désactive l'utilisation de la technologie iSwift.

Exemples :

- *Lancer l'analyse de la mémoire vive, des objets de démarrage automatique, des boîtes aux lettres et des répertoires My Documents, Program Files et du fichier test.exe :*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My
Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Analyser les objets dont la liste est reprise dans le fichier object2scan.txt. Utiliser le fichier de configuration scan_settings.txt. À la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Exemple de fichier de configuration :

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

MISE A JOUR DE L'APPLICATION

L'instruction pour la mise à jour des modules de Kaspersky Anti-Virus et des bases de l'application possède la syntaxe suivante :

```
avp.com UPDATE [<source_de_la_mise_à_jour>] [/R[A]:<fichier_de_rapport>]
[/C:<nom_du_fichier>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

<source_de_la_mise_à_jour>	Serveur HTTP, serveur FTP pou répertoire de réseau pour le chargement de la mise à jour. Ce paramètre accepte en tant que valeur le chemin d'accès complet à la source des mises à jour ou une URL. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.
/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants. **/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran ; portent sur tous les événements.
/C:<nom_du_fichier>	Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de Kaspersky Anti-Virus pour la mise à jour. Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour la mise à jour de l'application. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs des paramètres définies dans l'interface de l'application qui seront utilisées.

Exemples :

- *Mettre à jour les bases de l'application et consigner tous les éléments dans le rapport :*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Mettre à jour les modules de Kaspersky Anti-Virus en utilisant les paramètres du fichier de configuration updateapp.ini :*

```
avp.com UPDATE /C:updateapp.ini
```

Exemple de fichier de configuration :

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de l'instruction :

```
avp.com ROLLBACK [/R[A]:<fichier_de_rapport>][/password=<votre_mot_de_passe>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants. **/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran ; portent sur tous les événements.
<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface.

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

Exemple :

```
avp.com ROLLBACK /RA:rollback.txt/password=<votre mot de passe>
```

EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de l'instruction :

```
avp.com EXPORT <profil> <nom_du_fichier>
```

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

<profil>	Composant ou tâche dont les paramètres sont exportés. Le paramètre **<profil>** peut prendre n'importe quelle des valeurs indiquées au point "Administration des composants de l'application et des tâches".
<nom_du_fichier>	Chemin d'accès au fichier vers lequel sont exportés les paramètres de Kaspersky Anti-Virus. Vous pouvez indiquer un chemin relatif ou absolu. Le fichier de configuration est enregistré au format binaire (dat), si aucun autre format n'est indiqué ou si le format n'est pas précisé, et il peut être ensuite utilisé pour transférer les paramètres de l'application vers d'autres ordinateurs. De plus, vous pouvez enregistrer le fichier de configuration au format texte. Dans ce cas, ajoutez l'extension txt. N'oubliez pas que l'importation de paramètres de la protection depuis un fichier texte n'est pas prise en charge. Ce fichier peut être utilisé uniquement pour consulter les paramètres de fonctionnement principaux de Kaspersky Anti-Virus.

Exemple :

```
avp.com EXPORT RTP c:\settings.dat
```

IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de l'instruction :

```
avp.com IMPORT <nom_du_fichier > [/password=< votre_mot_de_passe >
```

La description des paramètres d'exécution de l'instruction est reprise dans le tableau ci-dessous.

<nom_du_fichier>	Chemin d'accès au fichier d'où sont importés les paramètres de Kaspersky Anti-Virus. Vous pouvez indiquer un chemin relatif ou absolu.
<votre_mot_de_passe>	Mot de passe pour Kaspersky Anti-Virus défini via l'interface de l'application. L'importation des paramètres de la protection est possible uniquement depuis un fichier au format binaire.

N'oubliez pas que l'instruction ne s'exécutera pas sans la saisie du mot de passe.

Exemple :

```
avp.com IMPORT c:\settings.dat /password=<mot de passe>
```

OBTENTION DU FICHIER DE TRACE

La création du fichier de trace s'impose parfois lorsque des problèmes se présentent dans le fonctionnement de Kaspersky Anti-Virus. Cela aidera les spécialistes du Support technique à détecter plus précisément les problèmes.

Il est conseillé d'activer la création de ces fichiers uniquement pour le diagnostic d'un problème particulier. L'activation permanente de cette fonction peut entraîner une réduction des performances de l'ordinateur et un débordement du disque dur.

Syntaxe de l'instruction :

```
avp.com TRACE [file] [on|off] [<niveau_de_trace>]
```

La description des paramètres est reprise dans le tableau ci-dessous.

[on|off]	Active/désactive la création d'un fichier de trace.
[file]	Réception de la trace dans un fichier.
<niveau_de_trace>	Pour ce paramètre, il est possible de saisir un chiffre compris entre 0 (niveau minimum, uniquement les événements critiques) et 700 (niveau maximum, tous les messages). Lorsque vous contactez le support technique, l'expert doit vous préciser le niveau qu'il souhaite. Si le niveau n'a pas été indiqué, il est conseillé d'utiliser la valeur 500.

Exemples :

- *Désactiver la constitution de fichiers de trace :*

```
avp.com TRACE file off
```

- *Créer un fichier de trace avec le niveau maximum de détails défini à 500 en vue d'un envoi à l'assistance technique :*

```
avp.com TRACE file on 500
```

CONSULTATION DE L'AIDE

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

```
avp.com [ /? | HELP ]
```

Pour obtenir de l'aide sur la syntaxe d'une instruction particulière, vous pouvez utiliser une des instructions suivantes :

```
avp.com <instruction> /?
avp.com HELP <instruction>
```

CODES DE RETOUR DE LA LIGNE DE COMMANDE

Cette section décrit les codes de retour de la ligne de commande (dans le tableau ci-dessous). Les codes généraux peuvent être renvoyés par n'importe quelle instruction de la ligne de commande. Les codes de retour des tâches concernent les codes généraux et les codes spécifiques à un type de tâche en particulier.

CODES DE RETOUR GENERAUX	
0	Opération réussie.
1	Valeur de paramètre invalide.
2	Erreur inconnue.
3	Erreur d'exécution de la tâche.
4	Annulation de l'exécution de la tâche.
CODES DE RETOUR DES TACHES D'ANALYSE ANTIVIRUS	
101	Tous les objets dangereux ont été traités.
102	Des objets dangereux ont été découverts.

LISTE DES NOTIFICATIONS DE KASPERSKY ANTI-VIRUS

Cette section reprend les informations sur les notifications qui peuvent être affichées sur l'écran pendant le fonctionnement de Kaspersky Anti-Virus.

DANS CETTE SECTION

NOTIFICATIONS DANS N'IMPORTE QUEL MODE DE PROTECTION

Cette section contient les informations relatives aux notifications qui s'affichent en mode de protection automatique et en mode de protection interactif (cf. section "Sélection du mode de protection" à la page 64).

DANS CETTE SECTION

UNE PROCEDURE SPECIALE DE REPARATION EST REQUISE

Suite à la découverte d'une menace active en ce moment dans le système (par exemple, un processus malveillant dans la mémoire vive ou dans les objets de démarrage), une notification vous invitant à lancer la procédure de réparation élargie s'affiche.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'objet. Le lien www.securelist.com (en Anglais) ou www.securelist.com/fr (en Français) dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.

- Le nom du fichier de l'objet malveillant, y compris son chemin d'accès.

Choisissez l'une des actions suivantes :

- **Oui, réparer et redémarrer** : exécute une procédure spéciale de réparation (recommandé).

  Lors de l'exécution de la procédure de réparation, l'exécution des applications est bloquée, sauf celle des applications de confiance. A l'issue de la réparation, le système d'exploitation redémarre, par conséquent avant de lancer la réparation, il est conseillé d'enregistrer tous les travaux en cours et de quitter toutes les applications. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète.

- **Ne pas exécuter** : l'objet ou le processus trouvé sera traité conformément aux actions sélectionnées précédemment.

Pour que l'application sélectionnée soit toujours appliquée quand une situation similaire se présente, cochez la case **Appliquer à tous les objets**.

UN DISQUE AMOVIBLE A ETE CONNECTE

Une notification apparaît lors de la connexion d'un disque amovible à l'ordinateur.

Choisissez l'une des actions suivantes :

- **Analyse rapide** : analyse les fichiers sur le disque amovible qui peuvent être potentiellement dangereux.
- **Analyse complète** : analyse tous les fichiers sur le disque amovible.
- **Ne pas analyser** : n'analyse pas le disque amovible.

Pour appliquer ultérieurement l'action sélectionnée à tous les disques amovibles à connecter, cochez la case **Appliquer à tous les cas similaires**.

UN CERTIFICAT DOUTEUX A ETE DECOUVERT

Kaspersky Anti-Virus analyse la sécurité de la connexion selon le protocole SSL à l'aide du certificat installé. En cas de tentative de connexion au serveur avec un certificat incorrect (par exemple, en cas de substitution du certificat par les individus malintentionnés), une notification s'affiche.

Le message reprend les informations suivantes :

- La description de la menace ;
- Le lien pour consulter le certificat ;
- Les causes possibles de l'erreur ;
- L'URL de la ressource.

Choisissez l'une des actions suivantes :

- **Oui, accepter le certificat douteux** : poursuit la connexion à une ressource en ligne.
- **Rejeter le certificat** : arrête la connexion à une ressource en ligne.

PROGRAMME DECOUVERT QUI POURRAIT ETRE UTILISE PAR L'INDIVIDU MALINTENTIONNE POUR NUIRE A L'ORDINATEUR OU AUX DONNEES DE L'UTILISATEUR

Quand la Surveillance du système détecte un programme qui pourrait être utilisé par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur, une notification s'affiche sur l'écran.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type et le nom du programme qui pourrait être utilisé par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.

  L'icône s'affiche à côté du nom de l'application. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'application.
- L'identificateur du processus et le nom du fichier de l'application, y compris le chemin d'accès.
- Le lien vers la fenêtre avec l'historique d'apparition de l'application.

Choisissez l'une des actions suivantes :

- **Autoriser** : autorise l'exécution de l'application.
- **Quarantaine** : quitte l'application ; place le fichier de l'application en quarantaine où il ne constituera pas de menace pour la sécurité de votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > Le statut du fichier, placé en quarantaine, peut être modifié lors d'une nouvelle analyse et devenir *sain*, mais, au plus tôt trois jours après la mise en quarantaine.

- **Terminer l'application** : interrompt l'exécution de l'application.
- **Ajouter aux exclusions** : autorise l'application à exécuter toujours de telles actions.

LE FICHIER EN QUARANTAINE N'EST PAS INFECTE

Kaspersky Anti-Virus analyse par défaut les fichiers en quarantaine après chaque mise à jour des bases. Si après l'analyse du fichier en quarantaine l'application détermine avec certitude qu'il est sain, une notification s'affiche.

Le message reprend les informations suivantes :

- recommandation sur la restauration du fichier qui se trouve en quarantaine ;
- nom du fichier, y compris le chemin d'accès au dossier dans lequel le fichier se trouvait avant d'être placé en quarantaine.

Choisissez l'une des actions suivantes :

- **Restaurer** : restaure le fichier en le supprimant de la quarantaine et en le replaçant dans le dossier où le fichier se trouvait avant la mise en quarantaine.
- **Annuler** : laisse l'objet en quarantaine.

UNE NOUVELLE VERSION DE L'APPLICATION EST DISPONIBLE

Quand une nouvelle version de Kaspersky Anti-Virus est disponible sur les serveurs de Kaspersky Lab, une notification apparaît.

Le message reprend les informations suivantes :

- Le lien vers les informations détaillées sur la nouvelle version de l'application ;
- La taille de la distribution.

Choisissez l'une des actions suivantes :

- **Oui, télécharger** : télécharge la distribution de la nouvelle version de l'application dans le dossier indiqué.
- **Non** : refuse de télécharger la distribution.

Pour que les notifications relatives aux nouvelles versions de l'application ne soient plus affichées, cochez la case **Ne pas m'informer de cette mise à jour**.

UNE MISE A JOUR TECHNIQUE A ETE DIFFUSEE

Quand une mise à jour technique de Kaspersky Anti-Virus est disponible sur les serveurs de Kaspersky Lab, une notification apparaît.

Le message reprend les informations suivantes :

- Le nouveau de la version de l'application installée sur l'ordinateur ;
- Le numéro de version de l'application après la mise à jour technique proposée ;
- Le lien vers les informations détaillées sur la mise à jour technique ;
- La taille du fichier de la mise à jour.

Choisissez l'une des actions suivantes :

- **Oui, télécharger** : charge le fichier de la mise à jour dans le dossier indiqué.
- **Non** : refuse de télécharger la mise à jour. Cette option est disponible si la case **Ne pas m'informer de cette mise à jour** a été cochée (cf. ci-après).
- **Non, me rappeler plus tard** : ne télécharge pas la mise à jour maintenant et envoi un rappel plus tard. Cette option est disponible si la case **Ne pas m'informer de cette mise à jour** a été décochée (cf. ci-après).

Pour que les notifications relatives à la mise à jour ne soient plus affichées, cochez la case **Ne pas m'informer de cette mise à jour**.

UNE MISE A JOUR TECHNIQUE A ETE TELECHARGEE

À l'issue du téléchargement de la mise à jour technique de Kaspersky Anti-Virus depuis les serveurs de Kaspersky Lab, une notification apparaît.

Le message reprend les informations suivantes :

- Le numéro de version de l'application après la mise à jour technique ;
- Le lien vers le fichier de la mise à jour.

Choisissez l'une des actions suivantes :

- **Oui, installer** : installe la mise à jour.

  Après l'installation de la mise à jour, il faut redémarrer le système d'exploitation.

- **Reporter l'installation** : reporte l'installation.

LA MISE A JOUR TECHNIQUE TELECHARGEE N'A PAS ETE INSTALLEE

Si une mise à jour technique de Kaspersky Anti-Virus a été téléchargée, mais pas encore installée, une notification apparaît.

Le message reprend les informations suivantes :

- Le numéro de version de l'application après la mise à jour technique ;
- Le lien vers le fichier de la mise à jour.

Choisissez l'une des actions suivantes :

- **Oui, installer** : installe la mise à jour.

  Après l'installation de la mise à jour, il faut redémarrer le système d'exploitation.

- **Reporter l'installation** : reporte l'installation.

Pour que les notifications sur cette mise à jour n'affichent plus, cochez la case **Ne pas demander jusqu'à l'apparition de la nouvelle version**.

VOTRE LICENCE EST EXPIREE

À l'échéance de la licence d'évaluation, Kaspersky Anti-Virus affiche une notification.

Le message reprend les informations suivantes :

- durée de la période d'évaluation ;
- informations sur les résultats du fonctionnement de l'application (peut inclure un lien pour l'affichage d'informations plus détaillées).

Choisissez l'une des actions suivantes :

- **Oui, acheter** : cette option ouvre une fenêtre du navigateur Internet et charge la page du magasin en ligne où il est possible d'acheter une licence commerciale pour l'utilisation de l'application.
- **Annuler** : refuser d'utiliser l'application. Si vous sélectionnez cette option, l'application cesse d'exécuter toutes les fonctions principales (recherche de virus, mise à jour, protection en temps réel, etc.).

LA MISE A JOUR DES BASES EST RECOMMANDEE AVANT L'ANALYSE

Lors du lancement de la tâche d'analyse avant ou pendant la première mise à jour des bases, une notification s'affiche sur l'écran.

Cette notification contient la recommandation d'actualiser les bases ou d'attendre la fin de la mise à jour avant l'analyse.

Choisissez l'une des actions suivantes :

- **Mettre à jour les bases avant l'analyse** : lancer la mise à jour des bases ; ensuite, la tâche d'analyse sera automatiquement lancée. Cette option est disponible si vous avez lancé la tâche d'analyse avant la première mise à jour des bases.
- **Lancer l'analyse après la mise à jour** : attendre la fin de la mise à jour des bases et lancer automatiquement la tâche d'analyse. Cette option est disponible si vous avez lancé la tâche d'analyse pendant la première mise à jour des bases.
- **Lancer l'analyse maintenant** : lancer la tâche d'analyse sans attendre la mise à jour des bases.

NOTIFICATIONS DANS LE MODE DE PROTECTION INTERACTIF

Cette section contient les informations relatives aux notifications qui s'affichent dans le mode de protection interactif (cf. section "Sélection du mode de protection" à la page 64).

DANS CETTE SECTION

UN OBJET SUSPECT/MALVEILLANT A ETE DECOUVERT.

Pendant le fonctionnement de l'Antivirus Fichiers, de l'Antivirus Courrier ou de la recherche de virus, un message s'affiche en cas de découverte d'un des objets suivants :

- objet malveillant ;
- objet contenant le code d'un virus inconnu ;
- objet contenant le code modifié d'un virus connu.

Le message reprend les informations suivantes :

- La description de la menace.

- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'objet. Le lien www.securelist.com (en Anglais) ou www.securelist.com/fr (en Français) dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.

- Le nom du fichier de l'objet malveillant, y compris son chemin d'accès.

Vous pouvez exécuter une des actions suivantes sur l'objet :

- **Réparer** : tentative de réparation de l'objet malveillant. Cette option est proposée quand la menace est connue.

  Une copie de sauvegarde de l'objet est créée avant la réparation.

- **Quarantaine** : place l'objet en quarantaine, où il ne constituera plus un danger pour votre ordinateur. Cette option est offerte si la menace et les méthodes de réparation de l'objet sont inconnues.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > Le statut du fichier, placé en quarantaine, peut être modifié lors d'une nouvelle analyse et devenir *sain*, mais, au plus tôt trois jours après la mise en quarantaine.

- **Supprimer** : supprime l'objet. Une copie de sauvegarde de l'objet est créée avant la suppression.

- **Ignorer/Bloquer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à toutes les menaces du même type découvertes pendant la session en cours du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les objets**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de Kaspersky Anti-Virus ainsi que la durée d'exécution de la tâche de recherche virale depuis son lancement jusqu'à la fin.

Si vous êtes convaincu que l'objet découvert n'est pas malveillant, il est conseillé de l'ajouté à la zone de confiance afin d'éviter une nouvelle réaction de l'application.

UNE VULNERABILITE A ETE DECOUVERTE

Une notification s'affiche en cas de découverte d'une vulnérabilité.

La notification contient les informations suivantes :

- La description de la vulnérabilité.

- Le nom de la vulnérabilité, tel qu'il figure dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur la vulnérabilité. Le lien www.securelist.com (en Anglais) ou www.securelist.com/fr (en Français) dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une vulnérabilité.

- Le nom du fichier de l'objet vulnérable, y compris son chemin d'accès.

Vous pouvez exécuter une des actions suivantes sur l'objet :

- **Oui, corriger** : supprime la vulnérabilité.
- **Ignorer** : n'exécute aucune action sur l'objet vulnérable.

UNE ACTIVITE DANGEREUSE A ETE DECOUVERTE DANS LE SYSTEME

Lorsque la Défense Proactive découvre une activité dangereuse en provenance d'une application quelconque du système, un message spécifique apparaît.

La notification contient les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'objet. Le lien www.securelist.com (en Anglais) ou www.securelist.com/fr (en Français) dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.
- L'identificateur du processus et le nom du fichier de l'application, y compris le chemin d'accès.

Choisissez l'une des actions suivantes :

- **Autoriser** : autorise l'exécution de l'application.
- **Quarantaine** : quitte l'application ; place le fichier de l'application en quarantaine où il ne constituera pas de menace pour la sécurité de votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > Le statut du fichier, placé en quarantaine, peut être modifié lors d'une nouvelle analyse et devenir *sain*, mais, au plus tôt trois jours après la mise en quarantaine.
- **Terminer l'application** : interrompt l'exécution de l'application.
- **Ajouter aux exclusions** : autorise l'application à exécuter toujours de telles actions.

Si vous êtes convaincu que l'application découverte ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky Anti-Virus.

REMISE A L'ETAT ANTERIEUR AUX MODIFICATIONS INTRODUITES PAR LE PROGRAMME QUI POURRAIT ETRE UTILISE PAR L'INDIVIDU MALINTENTIONNE POUR NUIRE A L'ORDINATEUR OU AUX DONNEES DE L'UTILISATEUR

Il est conseillé de revenir à l'état antérieur aux modifications introduites dans le système par le programme (annuler) qui pourrait être utilisé par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur. Une demande de confirmation de la remise à l'état antérieur s'affiche quand un tel programme s'arrête.

Le message reprend les informations suivantes :

- La demande sur la remise à l'état antérieur aux modifications introduites par le programme qui pourrait être utilisé par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.
- Le type d'application et son nom.

  L'icône s'affiche à côté du nom de l'application. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'application.
- L'identificateur du processus et le nom du fichier de l'application, y compris le chemin d'accès.

Choisissez l'une des actions suivantes :

- **Ignorer** : n'annule pas les modifications.
- **Oui, restaurer** : tente d'annuler les modifications introduites par l'application.

UN PROGRAMME MALVEILLANT A ETE DECOUVERT

Quand la Surveillance du système découvre une application dont le comportement correspond parfaitement à celui d'un programme malveillant, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de programme malveillant et son nom.

  L'icône s'affiche à côté du nom de l'application. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'application.
- L'identificateur du processus et le nom du fichier de l'application, y compris le chemin d'accès.
- Le lien vers la fenêtre avec l'historique d'apparition de l'application.

Choisissez l'une des actions suivantes :

- **Autoriser** : autorise l'exécution de l'application.
- **Quarantaine** : quitte l'application ; place le fichier de l'application en quarantaine où il ne constituera pas de menace pour la sécurité de votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > Le statut du fichier, placé en quarantaine, peut être modifié lors d'une nouvelle analyse et devenir *sain*, mais, au plus tôt trois jours après la mise en quarantaine.
- **Terminer l'application** : interrompt l'exécution de l'application.
- **Ajouter aux exclusions** : autorise l'application à exécuter toujours de telles actions.

PROGRAMME DECOUVERT QUE LES INDIVIDUS MALINTENTIONNES PEUVENT UTILISER

Si l'Antivirus Fichiers, l'Antivirus Courrier ou la tâche d'analyse sur les virus découvrent une application que les individus malintentionnés peuvent utiliser, une notification s'affiche sur l'écran.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'objet. Le lien www.securelist.com (en Anglais) ou www.securelist.com/fr (en Français) dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises.
- Le nom du fichier de l'objet, y compris son chemin d'accès.

Vous pouvez exécuter une des actions suivantes sur l'objet :

- **Quarantaine** : place l'objet en quarantaine, où il ne constituera plus un danger pour votre ordinateur. Cette option est offerte si la menace et les méthodes de réparation de l'objet sont inconnues.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > Le statut du fichier, placé en quarantaine, peut être modifié lors d'une nouvelle analyse et devenir *sain*, mais, au plus tôt trois jours après la mise en quarantaine.
- **Supprimer** : supprime l'objet. Une copie de sauvegarde de l'objet est créée avant la suppression.
- **Supprimer l'archive** : supprime l'archive protégée par un mot de passe.
- **Ignorer/Bloquer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).
- **Ajouter aux exclusions** : crée une règle d'exclusion pour ce type de menaces.

Pour appliquer l'action sélectionnée à toutes les menaces du même type découvertes pendant la session en cours du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les objets**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de Kaspersky Anti-Virus ainsi que la durée d'exécution de la tâche de recherche virale depuis son lancement jusqu'à la fin.

Si vous êtes convaincu que l'objet découvert n'est pas malveillant, il est conseillé de l'ajouté à la zone de confiance afin d'éviter une nouvelle réaction de l'application.

UN LIEN SUSPECT/MALVEILLANT A ETE DECOUVERT

Quand Kaspersky Anti-Virus détecte une tentative d'ouverture d'un site Web au contenu malveillant ou suspect, une notification s'affiche.

Le message reprend les informations suivantes :

- La description de la menace ;
- Le nom de l'application (du navigateur) à l'aide de laquelle le chargement du site Web est exécuté ;
- L'adresse du site ou de la page au contenu malveillant ou suspect.

Choisissez l'une des actions suivantes :

- **Autoriser** : poursuit le chargement du site Web.
- **Interdire** : bloque le chargement du site Web.

Pour appliquer l'action sélectionnée à tous les sites Web présentant la même menaces découverts dans la session en cours du composant de la protection, cochez la case **Appliquer à tous les objets**. La session de fonctionnement en cours d'un composant désigne la période entre le moment où il a été lancé et le moment où il est arrêté ou le redémarrage de Kaspersky Anti-Virus.

UN OBJET DANGEREUX A ETE DECOUVERT DANS LE TRAFIC

Lorsque l'Antivirus Internet découvre un objet dangereux dans le trafic, une notification s'affiche.

La notification contient les informations suivantes :

- La description de la menace ou des actions exécutées par l'application.
- Le nom de l'application en action.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône  s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'objet. Le lien www.securelist.com (en Anglais) ou www.securelist.com/fr (en Français) dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.
- Emplacement de l'objet (URL).

Choisissez l'une des actions suivantes :

- **Autoriser** : continue à télécharger l'objet.
- **Interdire** : bloque le téléchargement de l'objet depuis le site Internet.

Pour appliquer l'action sélectionnée à toutes les menaces du même type découvertes pendant la session en cours du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les objets**. La session de fonctionnement en cours d'un composant désigne la période entre le moment où il a été lancé et le moment où il est arrêté ou le redémarrage de Kaspersky Anti-Virus.

UNE TENTATIVE DE CONNEXION A UN SITE D'HAMEÇONNAGE (PHISHING) A ETE DECOUVERTE

Quand Kaspersky Anti-Virus détecte une tentative de connexion à un site qui est un site d'hameçonnage (phishing) confirmé ou potentiel, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace ;
- L'adresse du site Web.

Choisissez l'une des actions suivantes :

- **Autoriser** : poursuit le chargement du site Web.
- **Interdire** : bloque le chargement du site Web.

Pour appliquer l'action sélectionnée à tous les sites Web présentant la même menace découverts dans la session en cours de Kaspersky Anti-Virus, cochez la case **Appliquer à tous les objets**. La session de fonctionnement en cours d'un composant désigne la période entre le moment où il a été lancé et le moment où il est arrêté ou le redémarrage de Kaspersky Anti-Virus.

UNE TENTATIVE D'ACCES A LA BASE DE REGISTRES SYSTEME A ETE DECOUVERTE

Quand la Défense Proactive découvre une tentative d'accès aux clés de la base de registres système, une notification apparaît.

Le message reprend les informations suivantes :

- La clé du registre victime de la tentative d'accès ;
- Le nom du fichier du processus à l'origine de la tentative d'accès à la base de registres, y compris le chemin d'accès à celui-ci.

Choisissez l'une des actions suivantes :

- **Autoriser** : autorise une fois l'exécution de l'action dangereuse ;
- **Interdire** : bloque une fois l'exécution de l'action dangereuse.

Pour que l'action que vous avez sélectionnée soit exécutée à chaque tentative d'accès aux clés de la base de registre, cochez la case **Créer une règle**.

Si vous estimez que l'activité de l'application qui a envoyé une requête aux clés de la base de registre système n'est pas dangereuse, ajoutez-la à la liste des applications de confiance.

LA REPARATION DE L'OBJET EST IMPOSSIBLE

Dans certains cas, il est impossible de réparer l'objet : par exemple, si le fichier est endommagé à un tel point qu'il est impossible d'en supprimer le code malveillant ou de le restaurer complètement. De plus, la procédure de réparation ne peut être appliquée à certains types d'objets malveillants comme les chevaux de Troie. Si la réparation de l'objet est impossible, une notification s'affiche.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type de la menace et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom de l'objet malveillant. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur l'objet. Le lien www.securelist.com (en Anglais) ou www.securelist.com/fr (en Français) dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.

- Le nom du fichier de l'objet malveillant, y compris son chemin d'accès.

Choisissez l'une des actions suivantes :

- **Supprimer** : supprime l'objet. Une copie de sauvegarde de l'objet est créée avant la suppression.
- **Ignorer/Bloquer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).
- **Ajouter aux exclusions** : crée une règle d'exclusion pour ce type de menaces.

Pour appliquer l'action sélectionnée à toutes les menaces du même type découvertes pendant la session en cours du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les objets**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de Kaspersky Anti-Virus ainsi que la durée d'exécution de la tâche de recherche virale depuis son lancement jusqu'à la fin.

DETECTION DE PROCESSUS CACHES

Quand la Défense Proactive découvre un processus caché dans le système, une notification apparaît.

Le message reprend les informations suivantes :

- La description de la menace.
- Le type et le nom de la menace tel que repris dans l'Encyclopédie des virus de Kaspersky Lab.

  L'icône s'affiche à côté du nom. Cliquez sur cette icône pour ouvrir une fenêtre contenant des informations sur la menace. Le lien www.securelist.com (en Anglais) ou www.securelist.com/fr (en Français) dans la fenêtre permet d'accéder au site Web de l'Encyclopédie des virus et d'obtenir des informations plus précises sur une menace.
- Le nom du fichier du pilote, y compris son chemin d'accès.

Choisissez l'une des actions suivantes :

- **Quarantaine** : quitte le processus ; place le fichier du processus en quarantaine où il ne constituera pas de menace pour la sécurité de votre ordinateur.

  Lors des analyses suivantes de la quarantaine, l'état de l'objet peut se modifier. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > Le statut du fichier, placé en quarantaine, peut être modifié lors d'une nouvelle analyse et devenir *sain*, mais, au plus tôt trois jours après la mise en quarantaine.
- **Terminer** : interrompt le processus.
- **Autoriser** : autorise l'exécution du processus.

Pour appliquer l'action sélectionnée à toutes les menaces du même type découverte au cours de la session actuelle de la Défense Proactive, cochez la case **Appliquer à tous les cas similaires**. La session de fonctionnement en cours d'un composant désigne la période entre le moment où il a été lancé et le moment où il est arrêté ou le redémarrage de Kaspersky Anti-Virus.

Si vous êtes convaincu que le processus découvert ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky Anti-Virus.

GLOSSAIRE

A

Activation de l'application

L'application devient entièrement fonctionnelle. L'utilisateur doit avoir une licence pour activer l'application.

Analyse du trafic

Analyse en temps réel des objets transitant par tous les protocoles (exemple : HTTP, FTP etc.), à l'aide de la dernière version des bases.

Analyseur heuristique

Technologie d'identification des menaces non reconnues par les bases des applications de Kaspersky Lab. Celle-ci permet d'identifier les objets soupçonnés d'être infectés par un virus inconnu ou par une nouvelle modification d'un virus connu.

L'analyseur heuristique permet d'identifier jusqu'à 92% des nouvelles menaces. Ce mécanisme est assez efficace et entraîne rarement des faux positifs.

Les fichiers identifiés à l'aide de l'analyseur heuristique sont considérés comme des fichiers suspects.

Application incompatible

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui ne peut être administrée via Kaspersky Anti-Virus.

Archive

Fichier qui contient un ou plusieurs autres objets qui peuvent être des archives.

Attaque virale

Tentatives multiples d'infection d'un ordinateur par un virus.

B

Base des URL d'hameçonnage (phishing)

Liste des URL de sites identifiés par les experts de Kaspersky Lab comme des sites d'hameçonnage (phishing). La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

Base des URL suspectes

Liste des URL de sites dont le contenu pourrait constituer une menace. La liste est composée par les experts de Kaspersky Lab. Elle est actualisée régulièrement et est livrée avec l'application de Kaspersky Lab.

Bases

Les bases de données sont créées par les experts de Kaspersky Lab et elles contiennent une description détaillée de toutes les menaces informatiques qui existent à l'heure actuelle ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces sont découvertes.

Blocage d'un objet

Interdiction de l'accès d'applications tiers à l'objet. L'objet bloqué ne peut être lu, exécuté, modifié ou supprimé.

C

CERTIFICAT DU SERVEUR D'ADMINISTRATION

Certificat qui intervient dans l'authentification du serveur d'administration lors de la connexion à celui-ci de la console d'administration et de l'échange de données avec les postes client. Le certificat du serveur d'administration est généré lors de l'installation du serveur d'administration et il est enregistré sur ce serveur dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

COMPTEUR D'EPIDEMIE DE VIRUS

Modèle qui sert à prévenir les utilisateurs en cas de menace d'épidémie de virus. Le compteur d'épidémie de virus renferme un ensemble de paramètres qui déterminent un seuil d'activité de virus, les modes de diffusions et le texte des messages.

D

DEGRE D'IMPORTANCE DE L'EVENEMENT

Caractéristique de l'événement consigné dans le fonctionnement de l'application de Kaspersky Lab. Il existe 4 degrés d'importance:

Evénement critique.

Refus de fonctionnement.

Avertissement.

Information.

Les événements d'un même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

DUREE DE VALIDITE DE LA LICENCE

Durée pendant laquelle vous pouvez utiliser toutes les fonctions de l'application de Kaspersky Lab. Généralement, la durée de validité d'une licence est d'une année calendrier à partir de la date d'installation. Une fois que la durée de validité est écoulée, les fonctions de l'application sont bloquées : vous ne pourrez plus actualiser les bases de l'application.

E

EN-TETE

Informations contenues dans le début du fichier ou du message et qui offrent des données de faibles niveaux sur l'état et le traitement du fichier (message). En particulier, l'en-tête du courrier électronique contient des renseignements tels que les données de l'expéditeur, du destinataire et la date.

ETAT DE LA PROTECTION

Etat actuel de la protection qui définit le niveau de protection de l'ordinateur.

EXCLUSION

Objet exclu de l'analyse de l'application de Kaspersky Lab. Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple : un répertoire ou un programme), des processus ou des objets selon un type de menace conforme à la classification de l'encyclopédie des virus. Des exclusions peuvent être définies pour chaque tâche.

F

FAUX POSITIF

Situation qui se présente lorsqu'un objet sain est considéré par l'application de Kaspersky Lab comme étant infecté car son code évoque celui d'un virus.

FICHIER DE LICENCE

Fichier portant l'extension .key et qui est votre "clé" personnelle, indispensable au fonctionnement de l'application de Kaspersky Lab. Ce fichier sera inclus dans la boîte si vous avez achetez le logiciel chez un distributeur Kaspersky Lab. En revanche, il vous sera envoyé par email si le produit provient d'une boutique Internet.

FICHIERS COMPACTE

Fichier d'archivage contenant un programme de décompactage ainsi que des instructions du système d'exploitation nécessaires à son exécution.

FLUX NTFS ALTERNATIFS

Flux de données du système de fichiers NTFS (alternate data streams) prévus pour contenir des attributs complémentaires ou des informations relatives au fichier.

Chaque fichier dans le système de fichiers NTFS présente un ensemble de flux (streams). Un des flux renferme le contenu du fichier que nous pouvons voir une fois que le fichier a été ouvert. Les autres flux (alternatifs) sont prévus pour les méta-informations et garantissent, par exemple, la compatibilité du système NTFS avec d'autres systèmes tels que l'ancien système de fichiers Macintosh – Hierarchical File System (HFS). Les flux peuvent être créés, supprimés, enregistrés séparément, renommer ou lancer comme processus.

Les flux alternatifs peuvent être exploités par des individus malintentionnés dans le but de dissimuler l'envoi ou la réception de données de l'ordinateur.

I

INSTALLATION A L'AIDE D'UN SCRIPT DE LANCEMENT

Méthode d'installation à distance des applications de Kaspersky Lab qui permet d'associer le lancement d'une tâche d'installation à distance à un compte utilisateur particulier (ou à plusieurs comptes). Lorsque l'utilisateur s'enregistre dans le domaine, une tentative d'installation de l'application sur le poste client d'où s'est connecté l'utilisateur est lancée. Cette méthode est conseillée pour l'installation d'applications sur des ordinateurs fonctionnant sous Microsoft Windows 98/Me.

INTERCEPTEUR

Sous-composant de l'application chargé de l'analyse de certains types de messages électroniques. La sélection d'intercepteurs installés dépend du rôle ou de la combinaison de rôles de l'application.

K

KASPERSKY SECURITY NETWORK

Kaspersky Security Network (KSN) est un ensemble de services en ligne qui permet d'accéder à la base de connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. L'utilisation des données de Kaspersky Security Network permet à l'application de réagir plus rapidement aux nouvelles formes de menace, améliore l'efficacité de certains composants de la protection et réduit la probabilité de faux positifs.

L

LICENCE ACTIVE

Licence en cours d'utilisation par l'application de Kaspersky Lab. La licence détermine la durée de validité du fonctionnement complet de l'application ainsi que la politique de licence de l'application. L'application ne peut avoir qu'une application active à la fois.

LICENCE COMPLEMENTAIRE

Licence ajoutée pour le fonctionnement de l'application de Kaspersky Lab mais qui n'a pas été activée. La licence complémentaire entre en vigueur lorsque la licence active parvient à échéance.

LISTE DES URL ANALYSEES

Liste des masques et des URL soumises obligatoirement à la recherche d'objets malveillants par l'application de Kaspersky Lab.

LISTE DES URL AUTORISEES

Liste des masques et des URL dont l'accès n'est pas bloqué par l'application de Kaspersky Lab. La liste des adresses est composée par les utilisateurs lors de la configuration de l'application.

LISTE DES URL DE CONFIANCE

Liste des masques et URL dont le contenu est jugé fiable par l'utilisateur. L'application de Kaspersky Lab ne recherche pas la présence éventuelle d'objets malveillants dans les pages qui correspondent à un élément de la liste.

LISTE DES URL INTERDITES

Liste des masques et des URL dont l'accès est bloqué par l'application de Kaspersky Lab. La liste des adresses est composée par les utilisateurs lors de la configuration de l'application.

LISTE NOIRE DES LICENCES

Base de données contenant des informations relatives aux clés de licence Kaspersky Lab bloquées. Le contenu du fichier de la liste noire est mis à jour en même temps que les bases.

M

MASQUE DE FICHIER

Représentation du nom et de l'extension d'un fichier par des caractères génériques. Les deux caractères principaux utilisés à cette fin sont * et ? (où * représente n'importe quel nombre de n'importe quel caractère et ? représente un caractère unique). À l'aide de ces caractères, il est possible de représenter n'importe quel fichier. Attention ! le nom et l'extension d'un fichier sont toujours séparés par un point.

MASQUE DE SOUS-RESEAU

Le masque de sous-réseau et l'adresse réseau permettent d'identifier un ordinateur au sein d'un réseau informatique.

MESSAGE INDECENT

Message électronique contenant un vocabulaire vulgaire.

MESSAGE SUSPECT

Message qui ne peut être considéré comme indésirable de manière certaine mais dont l'analyse donne lieu à des soupçons (par exemple, certains types d'envois et de messages publicitaires).

MISE EN QUARANTAINE D'OBJETS

Mode de traitement d'un objet potentiellement infecté empêchant tout accès à celui-ci et engendrant son déplacement vers le dossier de quarantaine où il est conservé de manière cryptée afin de prévenir toute action malveillante.

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés sur les serveurs de mise à jour de Kaspersky Lab.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de garantir l'actualité de la protection. Dans ce scénario, les bases sont copiées depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et elles sont installées automatiquement.

MISE A JOUR DISPONIBLE

Ensemble de mises à jour des modules de l'application de Kaspersky Lab qui reprend les mises à jour urgentes rassemblées au cours d'un intervalle de temps défini ainsi que les modifications de l'architecture de l'application.

MISE A JOUR URGENTE

Mise à jour critique des modules de l'application de Kaspersky Lab.

MODULES LOGICIELS

Fichiers faisant partie de la distribution de l'application de Kaspersky Lab et responsables de ses principales tâches. Chaque type de tâche réalisée par l'application (Protection en temps réel, Analyse à la demande, Mise à jour) possède son propre module exécutable. En lançant l'analyse complète depuis la fenêtre principale, vous démarrez le module lié à cette tâche.

MODELE DE NOTIFICATION

Modèle utilisé pour signaler la découverte d'objets infectés lors de l'analyse. Le modèle de notification contient un ensemble de paramètres qui définissent l'ordre des notifications, les moyens de diffusion et le texte du message.

N

NIVEAU DE PROTECTION

Le niveau de protection est l'ensemble de paramètres prédéfinis de fonctionnement du composant.

NIVEAU RECOMMANDE

Niveau de protection qui repose sur les paramètres de fonctionnement définis par les experts de Kaspersky Lab et qui garantit la protection optimale de votre ordinateur. Ce niveau de protection est activé par défaut à l'installation.

O

OBJET OLE

Objet uni ou intégré à un autre fichier. L'application de Kaspersky Lab permet de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

OBJET CONTROLE

Fichier transmis via le protocole HTTP, FTP ou SMTP par le pare-feu et envoyé à l'application de Kaspersky Lab pour analyse.

OBJET DANGEREUX

Objet contenant un virus. Nous vous déconseillons de manipuler de tels objets car ils pourraient infecter votre ordinateur. Suite à la découverte d'un objet infecté, il est conseillé de le réparer à l'aide d'une application de Kaspersky Lab ou de le supprimer si la réparation est impossible.

OBJET INFECTE

Objet contenant un code malveillant : l'analyse de l'objet a mis en évidence une équivalence parfaite entre une partie du code de l'objet et le code d'une menace connue. Les experts de Kaspersky Lab vous déconseillent de manipuler de tels objets car ils pourraient infecter votre ordinateur.

OBJET INFECTE POTENTIELLEMENT

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus, mais inconnu de Kaspersky Lab. Les objets potentiellement infectés sont identifiés à l'aide de l'analyseur heuristique.

OBJET POTENTIELLEMENT INFECTE

Objet qui, en raison de son format ou de sa structure, peut être utilisé par un individu malintentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'infection par un code malveillant est très élevé pour ces fichiers.

OBJET SUSPECT

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus, mais inconnu de Kaspersky Lab. Les objets suspects sont détectés grâce à l'analyseur heuristique.

OBJETS DE DEMARRAGE

Série de programmes indispensables au lancement et au bon fonctionnement du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus qui s'attaquent en particulier à ces objets, ce qui peut par exemple provoquer le blocage du système d'exploitation.

OUTIL DE DISSIMULATION D'ACTIVITE

Programme ou ensemble de programmes qui permet de dissimuler la présence de l'individu malintentionné ou du programme malveillant dans le système.

Dans les systèmes Windows, on considère comme programme malveillant tout programme qui s'infiltre dans le système et intercepte les fonctions système (Windows API). L'interception et la modification de fonctions API de bas niveau permet avant tout à ce genre de programme de bien masquer sa présence dans le système. De plus, en général, un outil de dissimulation d'activité masque la présence dans le système de n'importe quel processus, répertoire ou fichier sur le disque ou clé de registre décrit dans sa configuration. De nombreux outils de dissimulation d'activité installent leurs pilotes et services dans le système (ils sont aussi invisibles).

P

PAQUET DE MISE A JOUR

Ensemble de fichiers copié depuis Internet et installés sur votre ordinateur afin de mettre à jour une application.

PARAMETRES DE L'APPLICATION

Paramètres de fonctionnement de l'application communs à tous les types de tâche, responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performance de l'application, les paramètres de création des rapports, les paramètres de la sauvegarde.

PARAMETRES DE LA TACHE

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

PASSERELLE A DEUX CANAUX

Ordinateur doté de deux cartes de réseau, chacune d'entre elles connectée à un réseau différent et transmettant les informations d'un réseau à l'autre.

PHISHING

Type d'escroquerie sur Internet qui consiste à envoyer aux victimes potentielles des messages électroniques, prétendument envoyés en général par une banque, dans le but d'obtenir des informations confidentielles.

PORT DE RESEAU

Paramètre des protocoles TCP et UDP déterminant la destination des paquets de données IP transmis vers l'hôte via le réseau et permettant aux divers programmes utilisés sur ce même hôte de recevoir des données indépendamment les uns des autres. Chaque programme traite les données envoyées sur un port bien défini (en d'autres termes, le programme "écoute" ce port).

Certains ports standards sont destinés aux protocoles réseau les plus courants (par exemple, les serveurs Web réceptionnent généralement les données envoyées via le protocole HTTP sur le port TCP 80). Néanmoins, un programme peut utiliser n'importe quel protocole et n'importe quel port. Valeurs possibles : de 1 à 65535.

PORT ENTREE-SORTIE

Utilisé dans les microprocesseurs (par exemple Intel) lors de l'échange de données avec les périphériques. Le port entrée-sortie est comparé à l'un ou l'autre périphérique et permet aux applications de le contacter pour l'échange de données.

PORT MATERIEL

Connexion pour un périphérique matériel quelconque via un câble ou une fiche (port LPT, port série, USB).

PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. Les objets lancés, ouverts ou conservés par un processus de confiance ne sont pas analysés.

PROTECTION EN TEMPS REEL

Mode de fonctionnement pendant lequel l'application recherche en temps réel la présence éventuelle de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

PROTOCOLE

Ensemble de règles clairement définies et standardisées, régulant l'interaction entre un client et un serveur. Parmi les protocoles les plus connus et les services liés à ceux-ci, on peut noter : HTTP (WWW), FTP et NNTP (news).

PROTOCOLE INTERNET (IP)

Protocole de base du réseau Internet, inchangé depuis son lancement en 1974. Il exécute les opérations principales liées au transfert de données d'un ordinateur à un autre et est à la base de protocoles de plus haut niveau tels que TCP et UDP. Il gère la connexion ainsi que la correction d'erreurs. Grâce à des technologies tels que le NAT et le masquerading, il est possible de dissimuler d'importants réseaux privés derrière quelques adresses IP (parfois même derrière une seule adresse). Cela permet de satisfaire la demande sans cesse croissante d'adresses IP alors que la plage IPv4 est relativement limitée.

Q

QUARANTAINE

Répertoire défini dans lequel sont placés tous les objets potentiellement infectés découverts pendant l'analyse ou par la protection en temps réel.

R

RESTAURATION

Déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

REPARATION D'OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration totale ou partielle des données ou sur le constat de l'impossibilité de réparer les objets. La réparation des objets s'opère sur la base des enregistrements des bases. Une partie des données peut être perdue lors de la réparation.

RÉPARATION D'OBJETS LORS DU REDÉMARRAGE

Mode de traitement des objets infectés utilisés par d'autres applications au moment de la réparation. Il consiste à créer une copie de l'objet infecté, à réparer cette copie et à remplacer l'objet original infecté par cette copie lors du redémarrage suivant de l'ordinateur.

S

SOCKS

Protocole de serveur proxy permettant une connexion à deux points entre des ordinateurs du réseau interne et des ordinateurs de réseaux externes.

SCRIPT

Petit programme informatique ou partie indépendante d'un programme (fonction) écrit, en règle générale, pour exécuter une petite tâche particulière. Ils interviennent le plus souvent lors de l'exécution de programmes intégrés à de l'hypertexte. Les scripts sont exécutés, par exemple, lorsque vous ouvrez certains sites Web.

Si la protection en temps réel est activée, l'application surveille l'exécution des scripts, les intercepte et vérifie s'ils contiennent des virus. En fonction des résultats de l'analyse, vous pourrez autoriser ou bloquer l'exécution du script.

SECTEUR D'AMORÇAGE DU DISQUE

Le secteur d'amorçage est un secteur particulier du disque dur de l'ordinateur, d'une disquette ou d'un autre support de stockage informatique. Il contient des informations relatives au système de fichiers du disque ainsi qu'un programme de démarrage s'exécutant au lancement du système d'exploitation.

Certains virus, appelés virus de boot ou virus de secteur d'amorçage, s'attaquent aux secteurs d'amorçage des disques. L'application de Kaspersky Lab permet d'analyser les secteurs d'amorçage afin de voir s'ils contiennent des virus et des les réparer en cas d'infection.

SERVEUR PROXY

Service dans les réseaux informatiques qui permet aux clients de réaliser des requêtes indirectes vers d'autres ressources du réseau. Le client se connecte d'abord au serveur proxy et envoi une requête vers une ressource quelconque (par exemple, un fichier) situé sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur indiqué et obtient la ressource demandée ou récupère la ressource dans son cache (si le serveur proxy possède son propre cache). Dans certains cas, la requête du client ou la réponse du serveur peuvent être modifiées par le serveur proxy à des fins déterminées.

SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Liste de serveurs HTTP et FTP de Kaspersky Lab d'où l'application peut récupérer les bases et les mises à jour des modules.

SERVICE DE NOMS DE DOMAINE (DNS)

Système distribué de traduction du nom d'hôte (ordinateur ou autre périphérique de réseau) en adresse IP. DNS fonctionne dans les réseaux TCP/IP. Dans certains cas particuliers, DNS peut enregistrer et traiter les requêtes de retour et définir le nom de l'hôte sur la base de son IP (enregistrement PTR). La résolution du nom DNS est généralement l'œuvre d'applications de réseau et non pas des utilisateurs.

SEUIL D'ACTIVITE VIRALE

Nombre d'événements d'un type donné et générés dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'un risque d'attaque virale. Ce paramètre est d'une importance capitale en cas d'épidémie de virus car il permet à l'administrateur d'anticiper l'attaque.

SUPPRESSION D'UN OBJET

Mode de traitement de l'objet qui entraîne sa suppression physique de l'endroit où il a été découvert par l'application (disque dur, répertoire, ressource de réseau). Ce mode de traitement est recommandé pour les objets dangereux dont la réparation est impossible pour une raison quelconque.

T

TECHNOLOGIE ICHECKER

Technologie qui permet d'accélérer l'analyse antivirus en excluant les objets qui n'ont pas été modifiés depuis l'analyse antérieure pour autant que les paramètres de l'analyse (bases antivirus et paramètres) n'aient pas été modifiés. Ces informations sont conservées dans une base spéciale. La technologie est appliquée aussi bien pendant la protection en temps réel que dans les analyses à la demande.

Admettons que vous possédez une archive qui a été analysée par une application de Kaspersky Lab et qui a reçu l'état sain. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases antivirus, l'archive sera analysée à nouveau.

Limitations technologiques d'iChecker :

La technologie ne fonctionne pas avec les fichiers de grande taille car dans ce cas il est plus rapide d'analyser tout le fichier que de vérifier s'il a été modifié depuis la dernière analyse ;

La technologie est compatible avec un nombre restreint de formats (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

TRAÇAGES

Exécution de débogage de l'application au cours duquel un arrêt a lieu après l'exécution de chaque étape afin d'en afficher les résultats.

TACHE

Fonctions exécutées par l'application de Kaspersky Lab sous la forme d'une tâche, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur, Mise à jour des bases.

V

VIDAGE DE LA MEMOIRE

Contenu de la mémoire active du processus ou de toute la mémoire vive du système à un moment donné.

VIRUS DE BOOT (AMORÇAGE)

Virus affectant les secteurs d'amorçage du disque de l'ordinateur. Au redémarrage du système, le virus force le système à inscrire en mémoire et à exécuter du code malveillant au lieu du code d'amorçage original.

VIRUS INCONNU

Nouveau virus au sujet duquel aucune information ne figure dans les bases. En règle générale, les virus inconnus sont découverts dans les objets à l'aide de l'analyse heuristique et ces objets reçoivent l'état potentiellement infecté.

KASPERSKY LAB

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire d'étude des virus :	newvirus@kaspersky.com
	(uniquement pour l'envoi d'objets suspects sous forme d'archive)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr
	(pour les questions aux experts de la lutte contre les virus)
Forum de Kaspersky Lab :	http://forum.kaspersky.com

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

INDEX

A

B

C

D

E

F

I

L

M

N

P

Q

R

S

T

Z